



# Trello

## Summary Report

Report created on April 09, 2024

Report date range: January 01, 2024 - March 31, 2024

Prepared by: Ben Howe, [bhowe@atlassian.com](mailto:bhowe@atlassian.com)



---

# Table of contents

|  |           |
|--|-----------|
| <b>Executive summary</b> .....         | <b>3</b>  |
| <b>Reporting and methodology</b> ..... | <b>4</b>  |
| Background .....                       | 4         |
| <b>Targets and scope</b> .....         | <b>5</b>  |
| Scope .....                            | 5         |
| <b>Findings Summary</b> .....          | <b>6</b>  |
| <b>Risk and priority key</b> .....     | <b>7</b>  |
| <b>Appendix</b> .....                  | <b>8</b>  |
| Submissions over time .....            | 8         |
| Submissions signal .....               | 8         |
| Bug types overview .....               | 9         |
| <b>Closing Statement</b> .....         | <b>10</b> |



---

# Executive summary

**Atlassian** engaged Bugcrowd, Inc. to perform a Bug Bounty Program, commonly known as a crowd-sourced penetration test.

A Bug Bounty Program is a cutting-edge approach to an application assessment or penetration test. Traditional penetration tests use only one or two personnel to test an entire scope of work, while a Bug Bounty leverages a crowd of security researchers. This increases the probability of discovering esoteric issues that automated testing cannot find and that traditional vulnerability assessments may miss in the same testing period.

The purpose of this program was to identify security vulnerabilities in the targets listed in the targets and scope section. Once identified, each vulnerability was rated for technical impact defined in the findings summary section of the report.

This report shows testing for **Trello's** targets during the period of: **01/01/2024 – 03/31/2024**.

For this Bug Bounty Program, submissions were received from **36** unique researchers.

The continuation of this document summarizes the findings, analysis, and recommendations from the Bug Bounty Program performed by Bugcrowd for **Atlassian**.

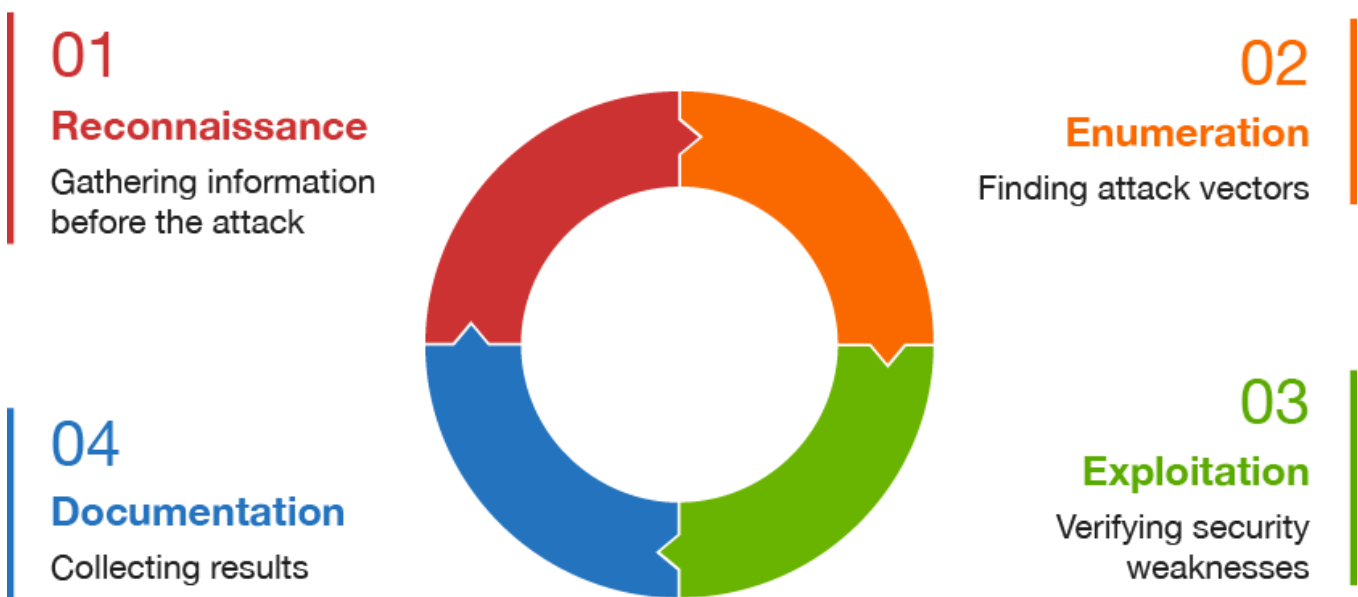
This report is a summary of the information available. All details of the engagement's findings — comments, code, and any tester provided remediation information — can be found in the [Bugcrowd platform \(https://tracker.bugcrowd.com\)](https://tracker.bugcrowd.com)

# Reporting and methodology

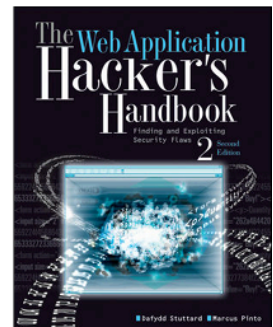
## Background

The strength of crowdsourced testing lies in multiple researchers, the pay-for-results model, and the varied methodologies that the researchers implement. To this end, researchers are encouraged to use their own individual methodologies on Bug Bounty Engagements.

The workflow of every penetration test can be divided into the following four phases:



Bugcrowd researchers who perform web application testing and vulnerability assessment usually subscribe to a variety of methodologies following the highlighted workflow, including the following:



---

# Targets and scope

## Scope

Prior to the Ongoing program launching, Bugcrowd worked with **Trello** to define the Rules of Engagement, commonly known as the program brief, which includes the scope of work. The following targets were considered explicitly in scope for testing:

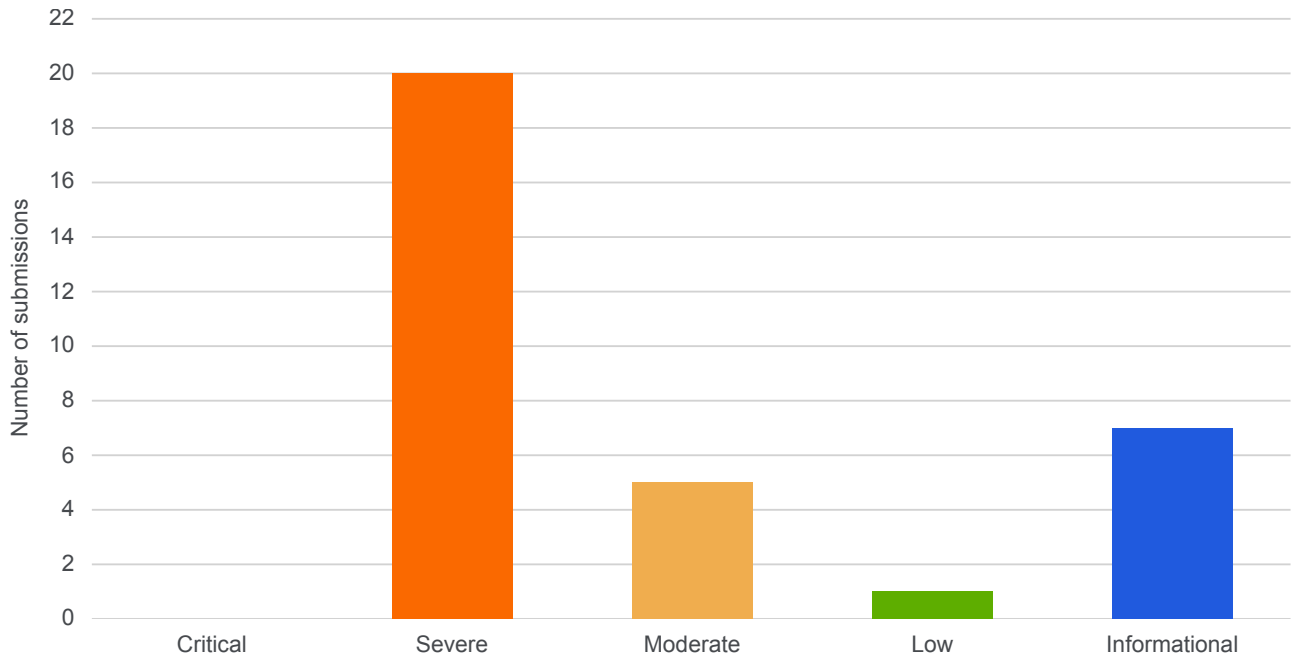
- trello.com
- api.trello.com
- \*.trello.services
- Trello Desktop Client
- Trello Mobile App for Android
- Trello Mobile App for iOS
- Butler for Trello
- Calendar Power-Up
- Card Aging Power-Up
- List Limits Power-Up
- Voting Power-Up
- Microsoft Teams Integration
- Trello Third Party Powerups

All details of the program scope and full program can be reviewed in the program settings.



# Findings Summary

The following chart shows all valid assessment findings from the program by technical severity.



# Risk and priority key

The following key is used to explain how Bugcrowd rates valid vulnerability submissions and their technical severity. As a trusted advisor Bugcrowd also provides common "next steps" for program owners per severity category.

## Technical severity

## Example vulnerability types

**Critical** **P1**

Critical severity submissions (also known as "P1" or "Priority 1") are submissions that are escalated to Bugcrowd as soon as they are validated. These issues warrant the highest security consideration and should be addressed immediately. Commonly, submissions marked as Critical can cause financial theft, unavailability of services, large-scale account compromise, etc.

- Remote Code Execution
- Vertical Authentication Bypass
- XML External Entities Injection
- SQL Injection
- Insecure Direct Object Reference for a critical function

**Severe** **P2**

High severity submissions (also known as "P2" or "Priority 2") are vulnerability submissions that should be slated for fix in the very near future. These issues still warrant prudent consideration but are often not availability or "breach level" submissions. Commonly, submissions marked as High can cause account compromise (with user interaction), sensitive information leakage, etc.

- Lateral authentication bypass
- Stored Cross-Site Scripting
- Cross-Site Request Forgery for a critical function
- Insecure Direct Object Reference for an important function
- Internal Server-Side Request Forgery

**Moderate** **P3**

Medium severity submissions (also known as "P3" or "Priority 3") are vulnerability submissions that should be slated for fix in the major release cycle. These vulnerabilities can commonly impact single users but require user interaction to trigger or only disclose moderately sensitive information.

- Reflected Cross-Site Scripting with limited impact
- Cross-Site Request Forgery for an important function
- Insecure Direct Object Reference for an unimportant function

**Low** **P4**

Low severity submissions (also known as "P4" or "Priority 4") are vulnerability submissions that should be considered for fix within the next six months. These vulnerabilities represent the least danger to confidentiality, integrity, and availability.

- Cross-Site Scripting with limited impact
- Cross-Site Request Forgery for an unimportant function
- External Server-Side Request Forgery

**Informational** **P5**

Informational submissions (also known as "P5" or "Priority 5") are vulnerability submissions that are valid but out-of-scope or are "won't fix" issues, such as best practices.

- Lack of code obfuscation
- Autocomplete enabled
- Non-exploitable SSL issues



## Bugcrowd's Vulnerability Rating Taxonomy

More detailed information regarding our vulnerability classification can be found at: <https://bugcrowd.com/vulnerability-rating-taxonomy>

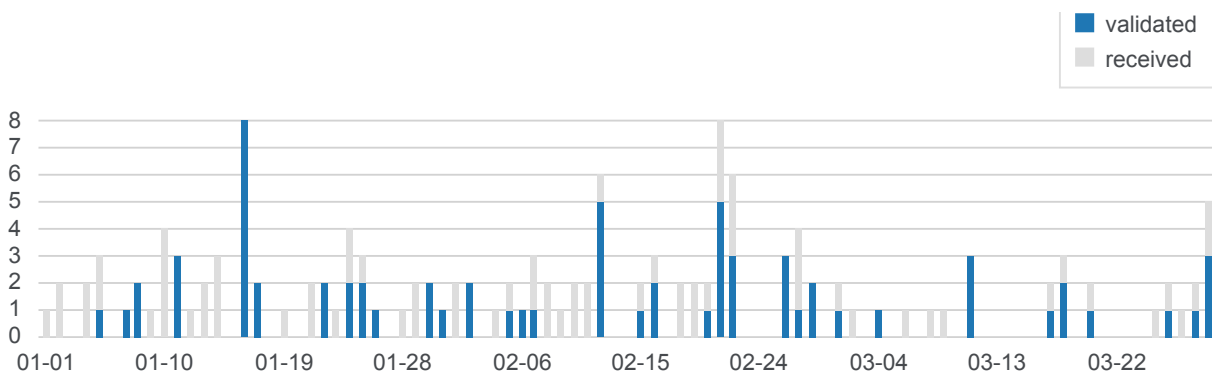


# Appendix

Included in this appendix are auxiliary metrics and insights into the Bug Bounty Program. This includes information regarding submissions over time, payouts and prevalent issue types.

## Submissions over time

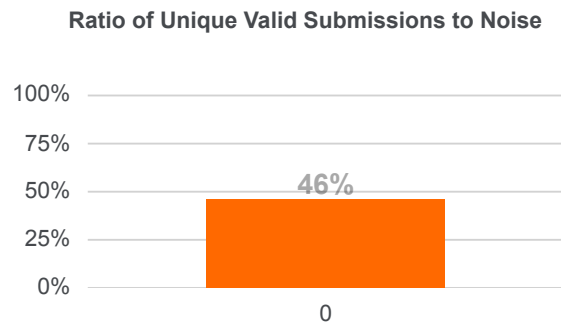
The timeline below shows submissions received and validated by the Bugcrowd team:



## Submissions signal

A total of **74** submissions were received, with **33** unique valid issues discovered. Bugcrowd identified **8** informational submissions, **15** duplicate submissions, removed **24** invalid submissions, and is processing **2** submissions. The ratio of unique valid submissions to noise was **46%**.

| Submission Outcome | Count     |
|--------------------|-----------|
| Valid              | 33        |
| Informational      | 8         |
| Invalid            | 24        |
| Duplicate          | 15        |
| Processing         | 2         |
| <b>Total</b>       | <b>74</b> |



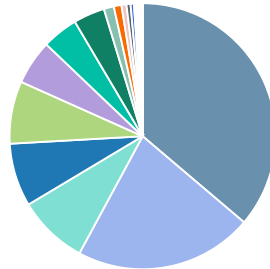




# Bug types overview

This distribution across bug types for the Bug Bounty Program only includes unique and valid submissions.

Average On-Demand Program



- Other
- Cross-Site Scripting (XSS)
- Server Security Misconfiguration
- Broken Access Control (BAC)
- Broken Authentication and Session Management
- Cross-Site Request Forgery (CSRF)
- Sensitive Data Exposure
- Server-Side Injection
- Unvalidated Redirects and Forwards
- Mobile Security Misconfiguration
- Application-Level Denial-of-Service (DoS)
- Insufficient Security Configurability
- Insecure Direct Object References (IDOR)
- Using Components with Known Vulnerabilities
- Missing Function Level Access Control
- Insecure OS/Firmware
- Insecure Data Storage
- Automotive Security Misconfiguration
- Insecure Data Transport
- Broken Cryptography
- Client-Side Injection
- Privacy Concerns
- External Behavior
- Lack of Binary Hardening
- Network Security Misconfiguration



---

# bugcrowd

Bugcrowd Inc.  
300 California St  
Suite 220 San Francisco, CA 94104  
(888)361-9734

**April 9 2024**

## Closing Statement

### Introduction

This report shows testing of **Trello** between the dates of **01/01/2024 - 03/31/2024**. During this time, **36** researchers from Bugcrowd submitted a total of **74** vulnerability submissions against Bugcrowd's targets. The purpose of this assessment was to identify security issues that could adversely affect the integrity of Bugcrowd. Testing focused on the following:

1. **trello.com**
2. **api.trello.com**
3. **\*.trello.services**
4. **Trello Desktop Client**
5. **Trello Mobile App for Android**
6. **Trello Mobile App for iOS**
7. **Butler for Trello**
8. **Calendar Power-Up**
9. **Card Aging Power-Up**
10. **List Limits Power-Up**
11. **Voting Power-Up**
12. **Microsoft Teams Integration**
13. **Trello Third Party Powerups**

The assessment was performed under the guidelines provided in the statement of work between Trello and Bugcrowd. This letter provides a high-level overview of the testing performed, and the result of that testing.



# Trello Program Overview

An Trello Program is a novel approach to a penetration test. Traditional penetration tests use only one or two researchers to test an entire scope of work, while an Ongoing program leverages a crowd of security researchers. This increases the probability of discovering esoteric issues that automated testing cannot find and that traditional vulnerability assessments may miss, in the same testing period.

It is important to note that this document represents a point-in-time evaluation of security posture. Security threats and attacker techniques evolve rapidly, and the results of this assessment are not intended to represent an endorsement of the adequacy of current security measures against future threats. This document contains information in summary form and is therefore intended for general guidance only; it is not intended as a substitute for detailed research or the exercise of professional judgment. The information presented here should not be construed as professional advice or service.

## Testing Methods

This security assessment leveraged researchers that used a combination of proprietary, public, automated, and manual test techniques throughout the assessment. Commonly tested vulnerabilities include code injection, cross-site request forgery, cross-site scripting, insecure storage of sensitive data, authorization/authentication vulnerabilities, business logic vulnerabilities, and more.

## Summary of Findings

During the Engagement, Bugcrowd discovered the following:

| Technical Severity                   | Count |
|--------------------------------------|-------|
| <b>Critical</b> vulnerabilities      | 0     |
| <b>Severe</b> vulnerabilities        | 20    |
| <b>Moderate</b> vulnerabilities      | 5     |
| <b>Low</b> vulnerability             | 1     |
| <b>Informational</b> vulnerabilities | 7     |