Trello
Trello keeps track of everything, from the big picture to the minute details.

Trello

Bugcrowd Ongoing program results

Report created on January 08, 2019

Report date range: October 01, 2018 - December 31, 2018

bugcrowd

Prepared by

bmarriott@atlassian.com

Table of contents

1 Executive summary **3**

2 Reporting and methodology **4**

Background 4

3 Targets and scope **5**

Scope 5

Team overview 5

4 Findings summary **6**

Findings by severity 6

Risk and priority key 7

5 Appendix **8**

Submissions over time 8

Submissions signal 8

Bug types overview 9

6 Closing statement **10**

Executive summary

bugcrowd

Trello engaged Bugcrowd, Inc. to perform an Ongoing Bounty Program, commonly known as a crowd-sourced penetration test.

An Ongoing 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 an Ongoing 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 engagement 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: **10/01/2018 – 12/31/2018**.

For this Ongoing Program, submissions were received from **61** unique researchers.

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

This report is just a summary of the information available.

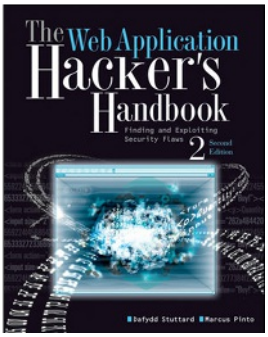
All details of the program's findings — comments, code, and any researcher provided remediation information — can be found in the Bugcrowd Crowdcontrol platform.

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 Bugcrowd Ongoing programs.

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:



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

CWE and SANS Institute
TOP 25 MOST DANGEROUS SOFTWARE ERRORS

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
```

All details of the program scope and full program brief can be reviewed in the Program Brief.

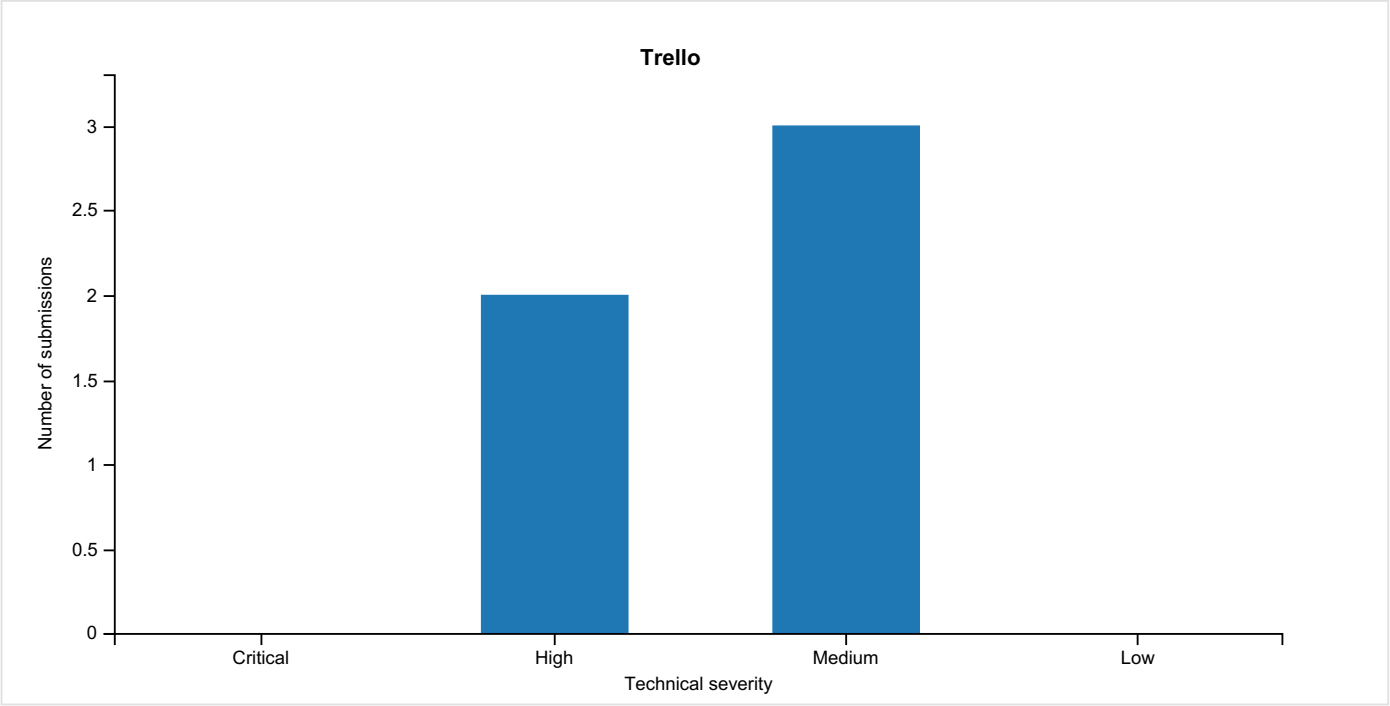
Team overview

The following Bugcrowd team members were assigned to this program:

TEAM ROLE	NAME
Application Security Engineer	Pawel Lesniewski
Application Security Engineer	Jonathan Jay Turla
Application Security Engineer	Trim Kadriu
Application Security Engineer	Sean Lawler
Application Security Engineer	Shpejtim Kurtishaj
Senior Director of Security Operations	Ryan Black
Senior Director of Customer Operations	Abby Mulligan

Findings by severity

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 Critical severity submissions (also known as "P1" or "Priority 1") are submissions that are escalated to **Trello** 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
High 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 a important function • Internal Server-Side Request Forgery
Medium 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 a important function • Insecure Direct Object Reference for an unimportant function
Low 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 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

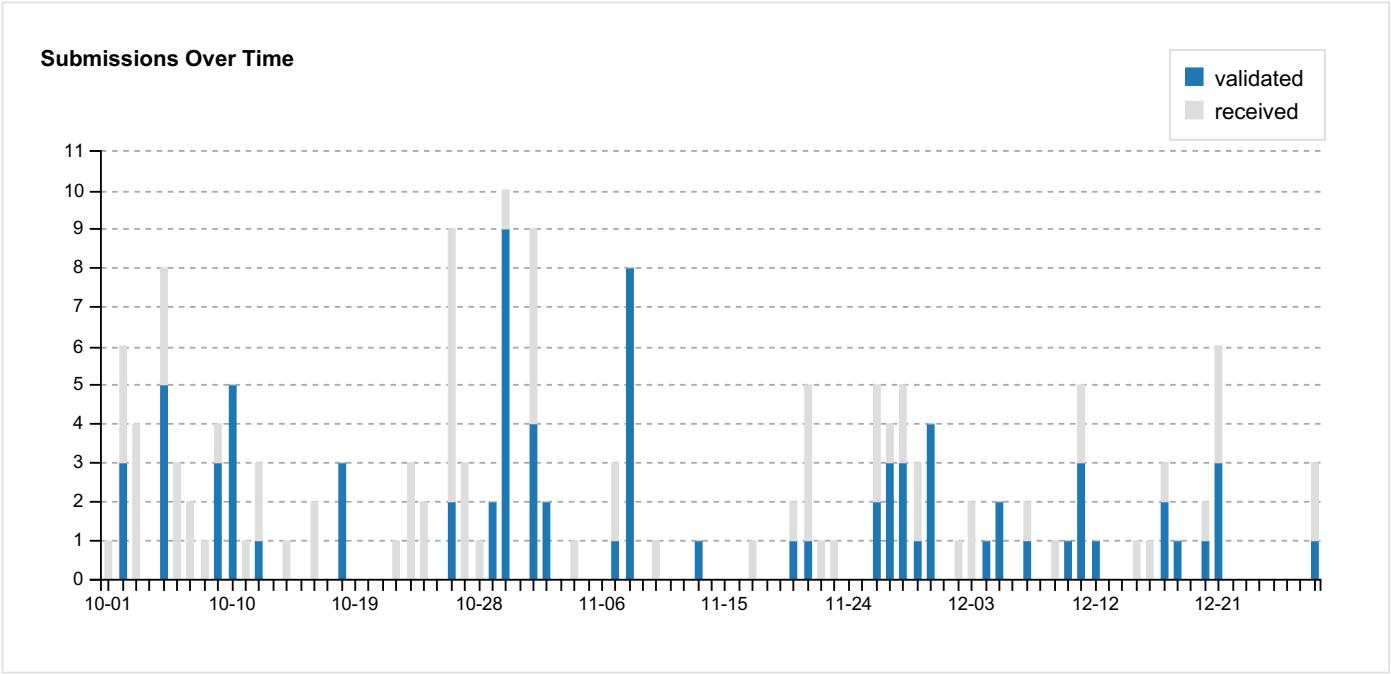
More detailed information regarding our vulnerability classification can be found at:
https://bugcrowd.com/vrt

Appendix

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

Submissions over time

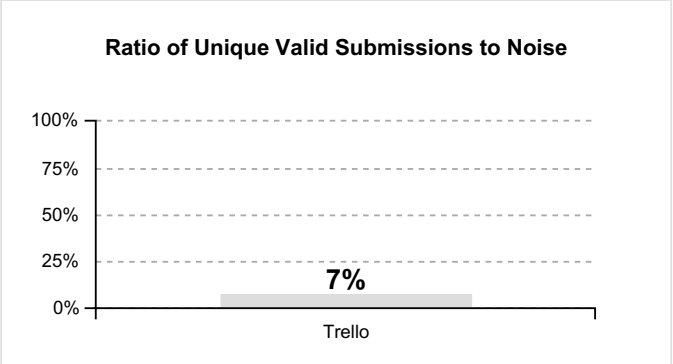
The timeline below shows submissions received and validated by the Bugcrowd team:



Submissions signal

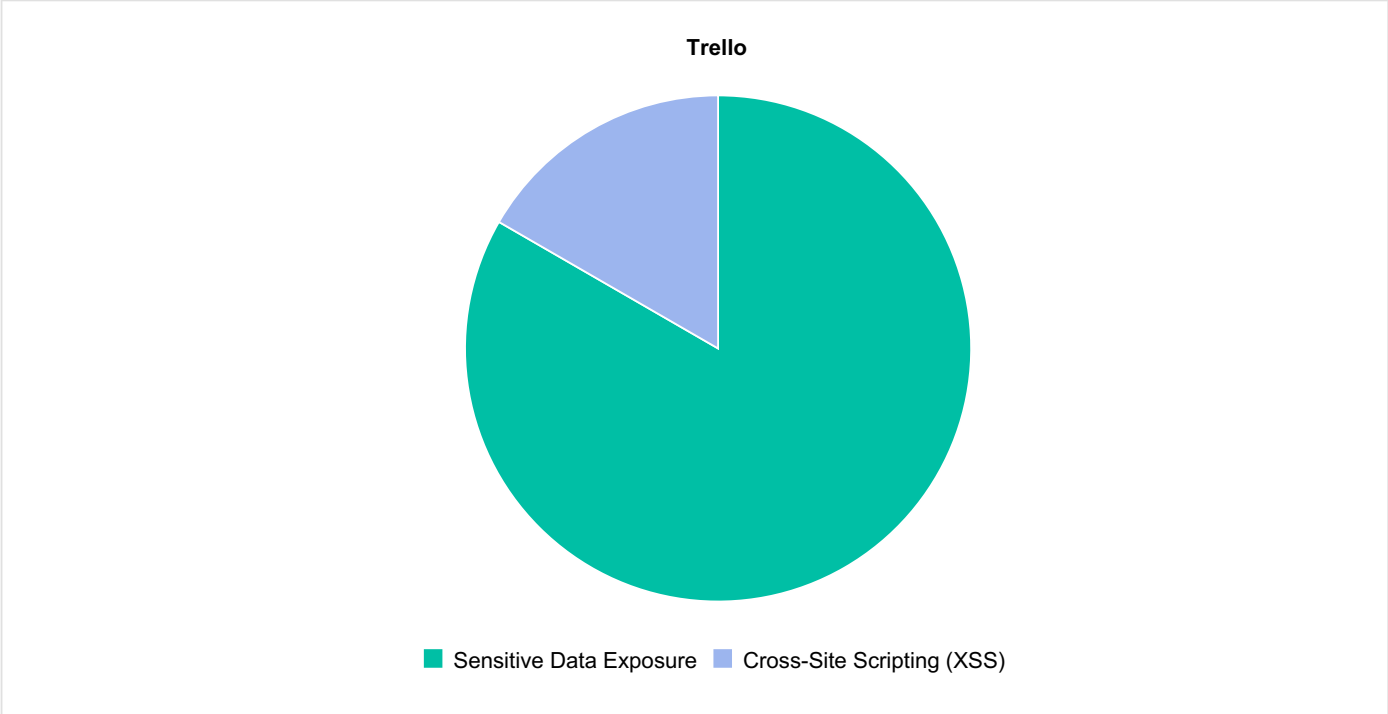
A total of **83** submissions were received, with **6** unique valid issues discovered. Bugcrowd identified **5** duplicate submissions, removed **72** invalid submissions, and is processing **0** submissions. The ratio of unique valid submissions to noise was **7%**.

SUBMISSION OUTCOME	COUNT
Valid	6
Invalid	72
Duplicate	5
Processing	0
Total	**83**



Bug types overview

The distribution of submissions across bug types for the Ongoing program is shown below.



Closing statement

bugcrowd

January 08, 2019

Bugcrowd Inc.
921 Front St
Suite 100
San Francisco, CA 94111

Introduction

This report shows testing of **Trello** between the dates of **10/01/2018 - 12/31/2018.** During this time, **61** researchers from Bugcrowd submitted a total of **83** vulnerability submissions against **Trello's** targets. The purpose of this assessment was to identify security issues that could adversely affect the integrity of Trello. Testing focused on the following:

1. **trello.com**
2. **api.trello.com**
3. ***.trello.services**

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.

Ongoing Program Overview

An Ongoing 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:

COUNT	TECHNICAL SEVERITY
0	Critical vulnerabilities
2	High vulnerabilities
3	Medium vulnerabilities
0	Low vulnerabilities
1	Informational finding