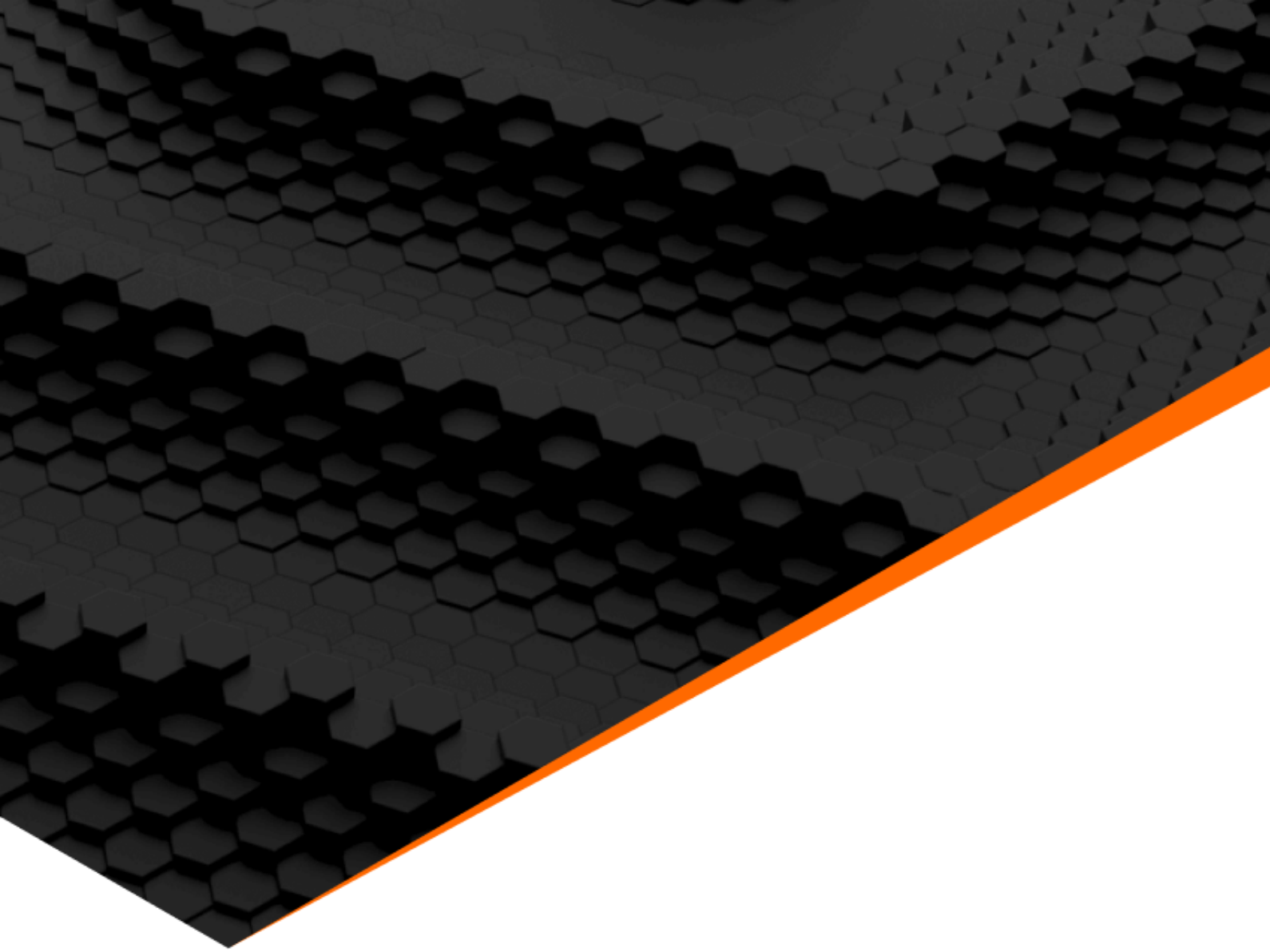


Release Management (by Y2 ENGR)

Summary Report

Report created on January 26, 2024
Report date range: January 01, 2022 - December 31, 2022
Prepared by: , yuri.lapin@releasemanagement.app

bugcrowd

Table of contents

Executive summary

Y2 ENGINEERING SP ZO.O. 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 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 **Release Management (by Y2 ENGR)'s** targets during the period of: **01/01/2022 – 12/31/2022**.

For this Ongoing Program, submissions were received from **8** unique researchers.

The continuation of this document summarizes the findings, analysis, and recommendations from the Ongoing Bounty Program performed by Bugcrowd for **Y2 ENGINEERING SP ZO.O.**.

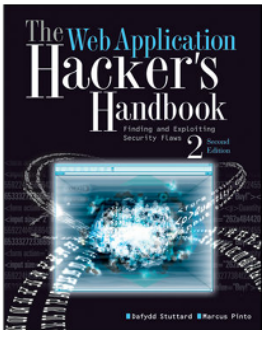
Reporting and methodology

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 Ongoing 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 **Release Management (by Y2 ENGR)** 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:

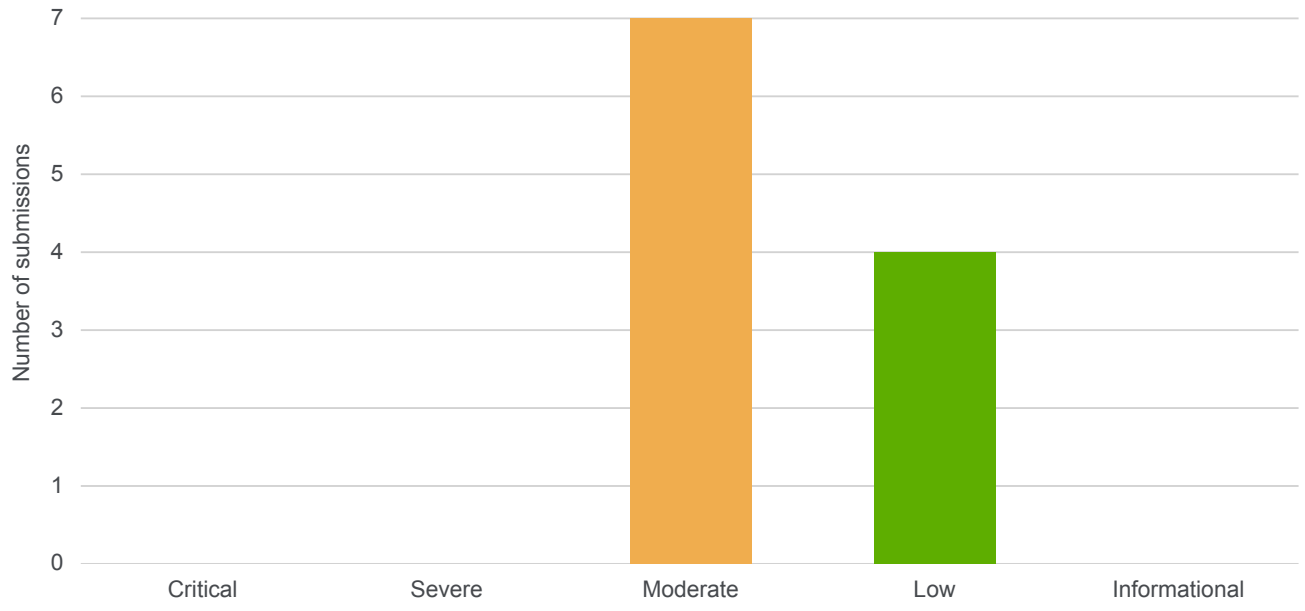
- Release Management & Roadmap -Jira Cloud - https://marketplace.atlassian.com/apps/1221946/release-management-roadmap-jira-cloud?hosting=cloud&tab=overview
- Gadgets for Release Management & Roadmap - Cloud - https://marketplace.atlassian.com/apps/1223487/gadgets-for-release-management-roadmap?hosting=cloud&tab=overview
- Gadgets for Release Management & Roadmap - DC - https://marketplace.atlassian.com/apps/1223487/gadgets-for-release-management-roadmap?hosting=datacenter&tab=overview
- Gadgets for Release Management & Road - Server - https://marketplace.atlassian.com/apps/1223487/gadgets-for-release-management-roadmap?hosting=server&tab=overview
- Advanced Agile Boards - Cloud - https://marketplace.atlassian.com/apps/1223877/advanced-agile-boards?hosting=cloud&tab=overview
- https://marketplace.atlassian.com/apps/1222474/work-status-time-tracking-calendar-for-jira?tab=overview&hosting=cloud
- https://marketplace.atlassian.com/apps/1228657/easy-peasy-roadmap-for-jira?hosting=cloud&tab=overview

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

https://tracker.bugcrowd.com/releasemanagement/settings/details

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

VRT

Bugcrowd's Vulnerability Rating Taxonomy

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

Findings table

The following table lists all valid assessment findings from the program / engagement

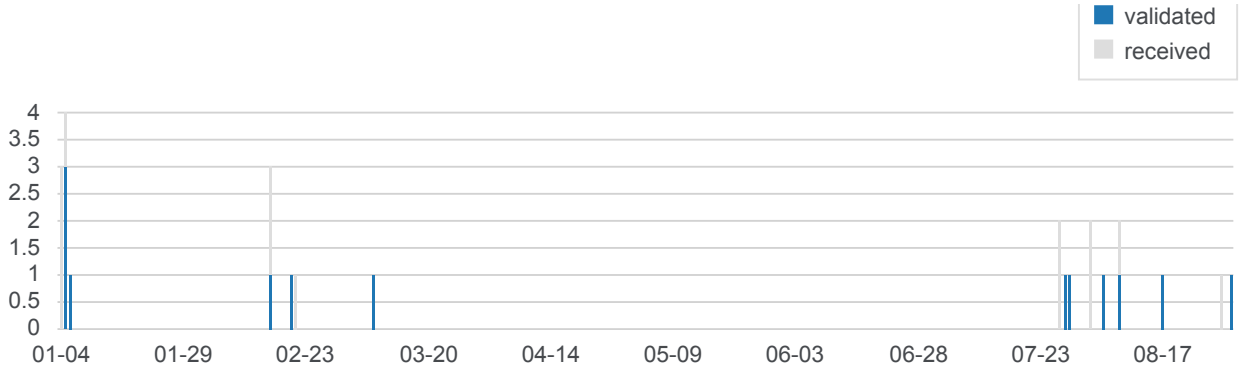
Title	VRT	Duplicates	Priority	State	Link
Stored XSS in issue name	Cross-Site Scripting (XSS)	-	P3	Resolved	
SSRF lead to leak of Amazon server /meta-data/	Broken Access Control (BAC)	-	P3	Resolved	
[Stored] XSS via Issue Summary in Notes functionality	Cross-Site Scripting (XSS)	-	P3	Resolved	
[Stored] XSS via Issue Field Name in Error Message modal	Cross-Site Scripting (XSS)	-	P3	Resolved	
Stored XSS at [issues calendar board] via [issues description filed]	Cross-Site Scripting (XSS)	-	P3	Resolved	
Leaked restricted [Projects] to Un-authorized user	Broken Access Control (BAC)	-	P3	Resolved	
Leaked restricted [Sprint] to Un-authorized user at [Calendar]	Broken Access Control (BAC)	-	P3	Resolved	
Non-admins can add non-working days to a board	Broken Authentication and Session Management	-	P4	Resolved	
Users without access to a private project can overwrite board settings for that project	Broken Authentication and Session Management	-	P4	Resolved	
Users without access to a private project can read/write comment on its version if the board is shared with them	Broken Access Control (BAC)	-	P4	Resolved	
Blind SSRF in webhooks	Broken Access Control (BAC)	-	P4	Resolved	
Unauthorised (Non-admin) User can change calendar.settings for projects that he don't have access to	Broken Authentication and Session Management	-	-	Informational	

Appendix

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

Submissions over time

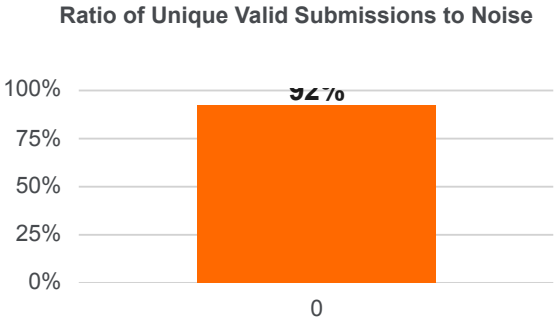
The timeline below shows submissions received and validated by the Bugcrowd team:



Submissions signal

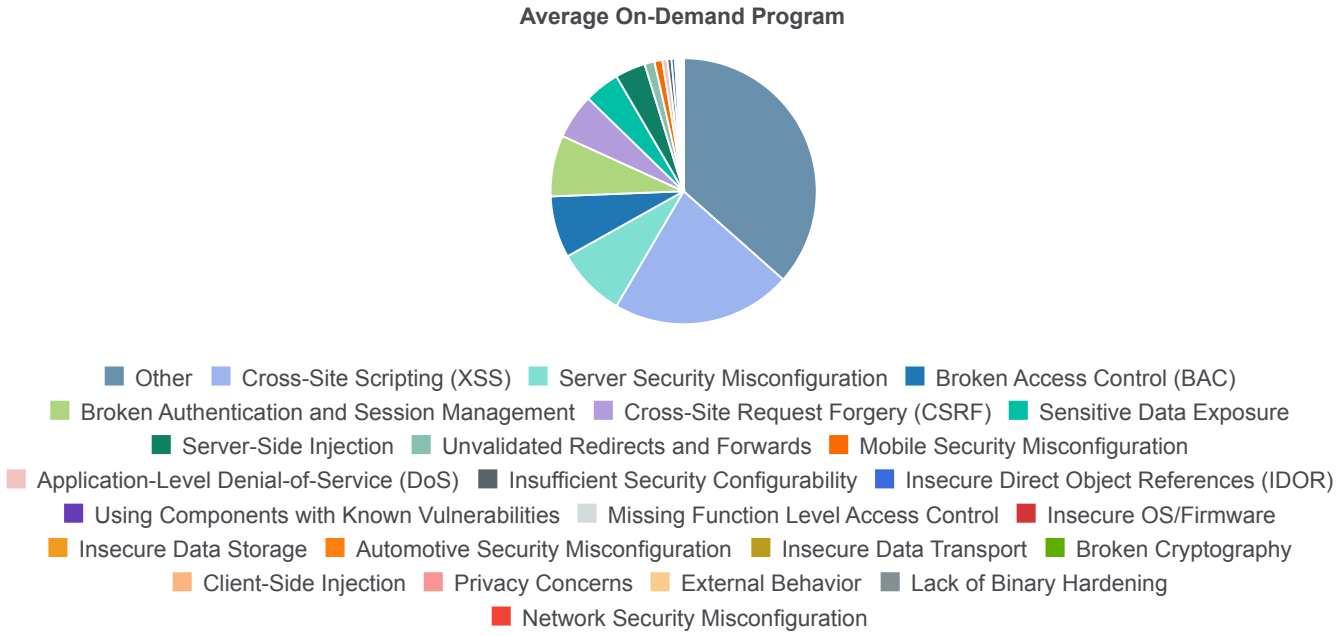
A total of **13** submissions were received, with **12** unique valid issues discovered. Bugcrowd identified **1** informational submissions, **1** duplicate submissions, removed **0** invalid submissions, and is processing **0** submissions. The ratio of unique valid submissions to noise was **92%**.

Submission Outcome	Count
Valid	12
Informational	1
Invalid	0
Duplicate	1
Processing	0
Total	**13**



Bug types overview

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



Spend of program rewards pool

During this Ongoing Bug Bounty Program, about **34%** of the total allocated reward pool of **$8,001** was paid. A number of other statistics regarding the Ongoing Bug Bounty Engagement's payouts are shown below.

$2,700.00 Total paid out to Researchers	**$2,700.00** Total to be paid to Researchers	**$1,901.00** Remaining prize pool
$300.00 Highest paid reward	**$100.00** Lowest paid reward	**$225.00** Average reward

Top 3 highest paid submissions

Title	Reward
[Stored] XSS via Issue Summary in Notes functionality 196dfcc5-338a-40f5-9571-6c852ea754c1	$300.00
SSRF lead to leak of Amazon server /meta-data/ 1e29b1de-c4ef-4478-a84e-cab338617a38	$300.00
[Stored] XSS via Issue Field Name in Error Message modal 46826b84-02a2-42e5-81f7-2c38c98c2cc9	$300.00

Bugcrowd Inc.
921 Front St
Suite 100 San Francisco, CA 94111
(888)361-9734

January 26 2024

Closing Statement

Introduction

This report shows testing of **Release Management (by Y2 ENGR)** between the dates of **01/01/2022 - 12/31/2022**. During this time, **8** researchers from Bugcrowd submitted a total of **13** 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. **Release Management & Roadmap -Jira Cloud - https://marketplace.atlassian.com/apps/1221946/release-management-roadmap-jira-cloud?hosting=cloud&tab=overview**
2. **Gadgets for Release Management & Roadmap - Cloud - https://marketplace.atlassian.com/apps/1223487/gadgets-for-release-management-roadmap?hosting=cloud&tab=overview**
3. **Gadgets for Release Management & Roadmap - DC - https://marketplace.atlassian.com/apps/1223487/gadgets-for-release-management-roadmap?hosting=datacenter&tab=overview**
4. **Gadgets for Release Management & Road - Server - https://marketplace.atlassian.com/apps/1223487/gadgets-for-release-management-roadmap?hosting=server&tab=overview**
5. **Advanced Agile Boards - Cloud - https://marketplace.atlassian.com/apps/1223877/advanced-agile-boards?hosting=cloud&tab=overview**
6. **https://marketplace.atlassian.com/apps/1222474/work-status-time-tracking-calendar-for-jira?tab=overview&hosting=cloud**
7. **https://marketplace.atlassian.com/apps/1228657/easy-peasy-roadmap-for-jira?hosting=cloud&tab=overview**

The assessment was performed under the guidelines provided in the statement of work between Release Management (by Y2 ENGR) and Bugcrowd. This letter provides a high-level overview of the testing performed, and the result of that testing.

Release Management (by Y2 ENGR) Program Overview

An Release Management (by Y2 ENGR) 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 Ongoingprogram 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
Critical vulnerabilities	0
Severe vulnerabilities	0
Moderate vulnerabilities	7
Low vulnerabilities	4
Informational vulnerabilities	0