INSTRUCTURE

PENETRATION TEST REPORT

JANUARY 1, 2021 – DECEMBER 31, 2021

Instructure Engineering, Security, and Operations

April 2022

Table of Contents

INSTRUCTURE

Executive Summary

Dear customers,

I am pleased to present Instructure's 11th annual open security audit. Once again, Instructure engaged Bugcrowd, Inc. to perform our Ongoing Bounty Program, commonly known as a crowd-sourced penetration test for its products. Simply put, we want to be as transparent about the programs and protocols we use to detect bugs and prevent badness wherever we possibly can. In fact, we are one of the only companies in the EdTech space to make our security audit available to customers, both publicly on our website and directly when requested.

In a nutshell, our security program is built based on ISO 27001, NIST's Cyber Security Framework, AICPA's Trust Services Principles and Criteria, and SANS' CIS Critical Security Controls. And we develop our applications abiding with OWASP's Top 10. We implement both preventative and detective mechanisms, as well as processes, controls, and tools in layers—helping to mitigate risks that might impact data, people, systems, operations, products, and our mission as a company.

The purpose of our Ongoing Bounty Program and penetration testing is to identify security vulnerabilities in the targets listed in the targets and scope section of this report. Once identified, each vulnerability was rated for technical impact defined in the findings summary section of the report.

The following report shows testing for Canvas LMS, Studio, Catalog, Commons, and Student Pathways. New this year is the addition of Mastery Connect. Bridge (which Instructure sold in early 2021), and Enterprise targets are also included. This report covers the full 2021 year during the period of: **01/01/2021 – 12/31/2021**. For this year's ongoing program, **166** submissions were received from **53** unique researchers.

As always, we appreciate all security concerns that are brought to light and we are constantly striving to keep on top of the latest threats. Being proactive rather than reactive to emerging security issues is a fundamental belief at Instructure. I would like to take this opportunity to thank the Bugcrowd community's efforts in creating a more secure world, and we are excited to see what you continue to discover. Thank you for helping us improve our applications and helping make our software more secure for end users.

Keep learning,

Roshan Popal

Roshan Popal,
Chief Information Officer (CIO), Instructure

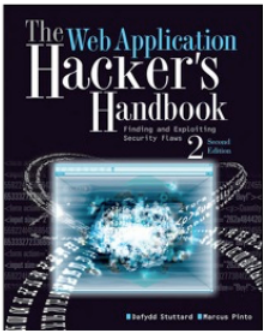
Reporting and Methodology

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.

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.

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

Program Overview

Our 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.

To help get Bugcrowd security researchers started, we provide Checkmarx outputs and staging environments of our products. The goal of this self-disclosure - along with transparency - is to reveal potential issues in our code base that may help a researcher find issues in our live applications. By reviewing this scanned output, a security researcher can gain a much deeper understanding of where vulnerabilities may be, and an easier time exploiting those issues for reward. Naturally, since this is source code scan results, some findings may not be exploitable due to other protections in place. Findings utilizing this scan output will be rewarded at the full normal amounts, of which details can be found at: https://bugcrowd.com/canvasbridgeinstructure

For anyone interested in joining our bug bounty program as a security researcher, please contact security@instructure.com with your Bugcrowd username and we will be pleased to add you to the research team.

Targets and Scope

Prior to the Ongoing program launching, Bugcrowd worked with Instructure 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:

Canvas LMS

```
https://bugcrowd-tc.instructure.com
```

Canvas Mobile

```
iOS App: Canvas Student
iOS App: Polls for Canvas
iOS App: Canvas Teacher
iOS App: Canvas Parent
Android App: Canvas Student (com.instructure.candroid)
Android App: Polls for Canvas
Android App: Canvas Teacher (com.instructure.teacher)
Android App: Canvas Parent (com.instructure.parentapp)
```

Canvas Commons

```
https://commons-pdx-edge.inseng.net
```

Canvas Catalog

```
https://catalog-bugcrowd.inscloudgate.net
```

Canvas Studio

```
https://sectest.beta.instructuremedia.com
```

Canvas Student Pathways

```
https://*.qa.ops.portfolium.net
```

Mastery Connect

```
https://*.masteryconnect-security.com/
Android App: MasteryConnect Teacher (com.masteryconnect.teacher)
```

Bridge Suite (legacy)*

```
https://*.suite.staging.bridgeapp.com
https://bugcrowd*.staging.bridgeapp.com
https://bugcrowd*.perform.stage.bridgeapp.com
https://*.stage.practice.xyz
```

**The sale of Bridge was completed in February 2021 to a third party and is no long an Instructure product.*

Other (Enterprise Issues)

Included in the Bugcrowd security program is enterprise testing of our own security program, platforms, and infrastructure.

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.

Bugcrowd's Vulnerability Rating Taxonomy

Technical Severity	Example Vulnerability Types
Critical Critical severity submissions (also known as "P1" or "Priority 1") are submissions that are escalated to Instructure 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.	• 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 an 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 an 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

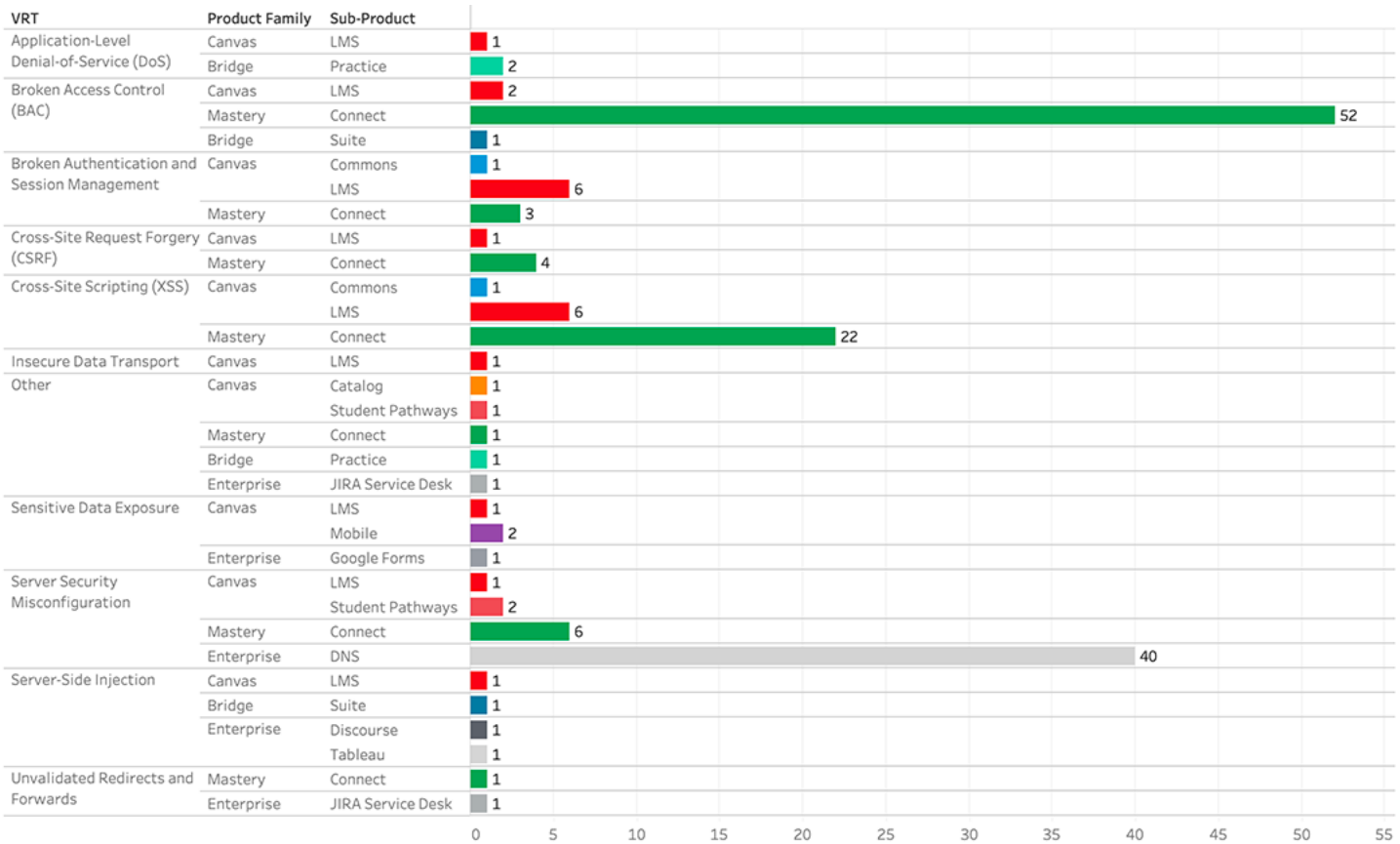
Findings Summary

During the program, Bugcrowd researchers discovered the following:

Priority	Canvas	Mastery	Bridge	Enterprise	Priority Total
Critical	1	2	1	2	**6**
High	5	15	0	4	**24**
Medium	15	59	2	26	**102**
Low	6	12	2	13	**33**
Informational	1	0	0	0	**1**
Product Total	**28**	**88**	**5**	**45**	**166**

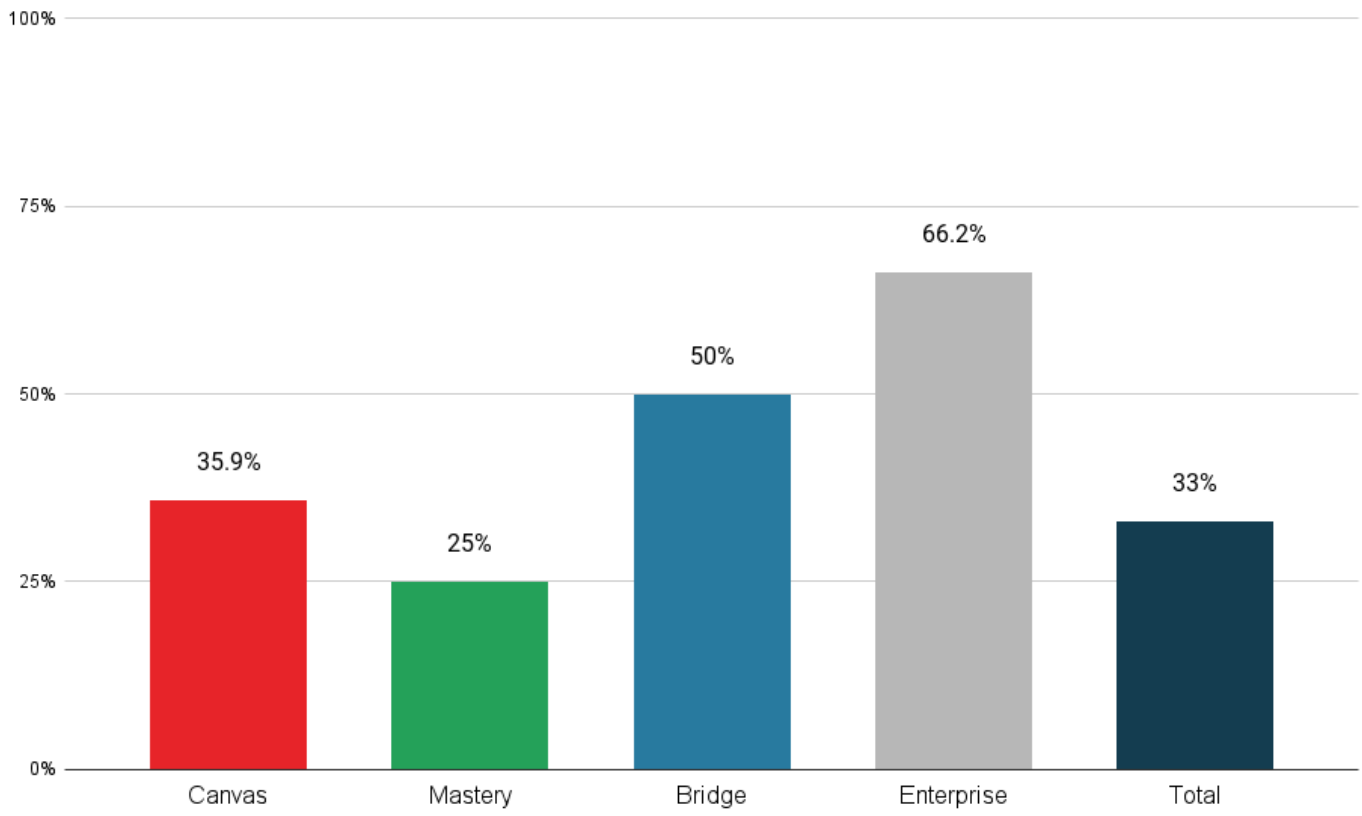
Bug Types Overview

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

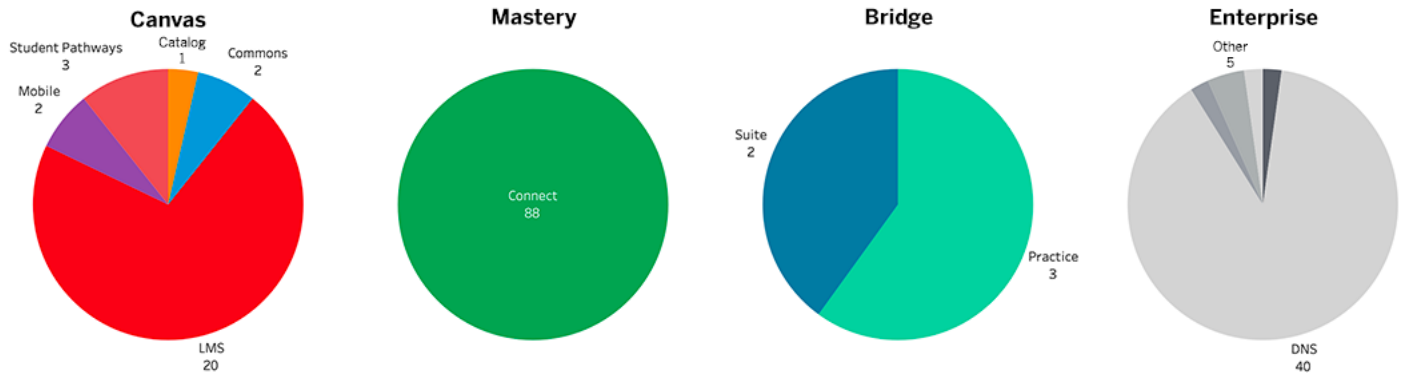


Submissions Signal

A total of **481** submissions were received, with **155** unique valid issues discovered. Bugcrowd identified **6** informational submissions, **89** duplicate submissions, removed **231** invalid submissions, and as of report publishing is processing **0** submissions. The ratio of unique valid submissions to noise was **33%** across all products.



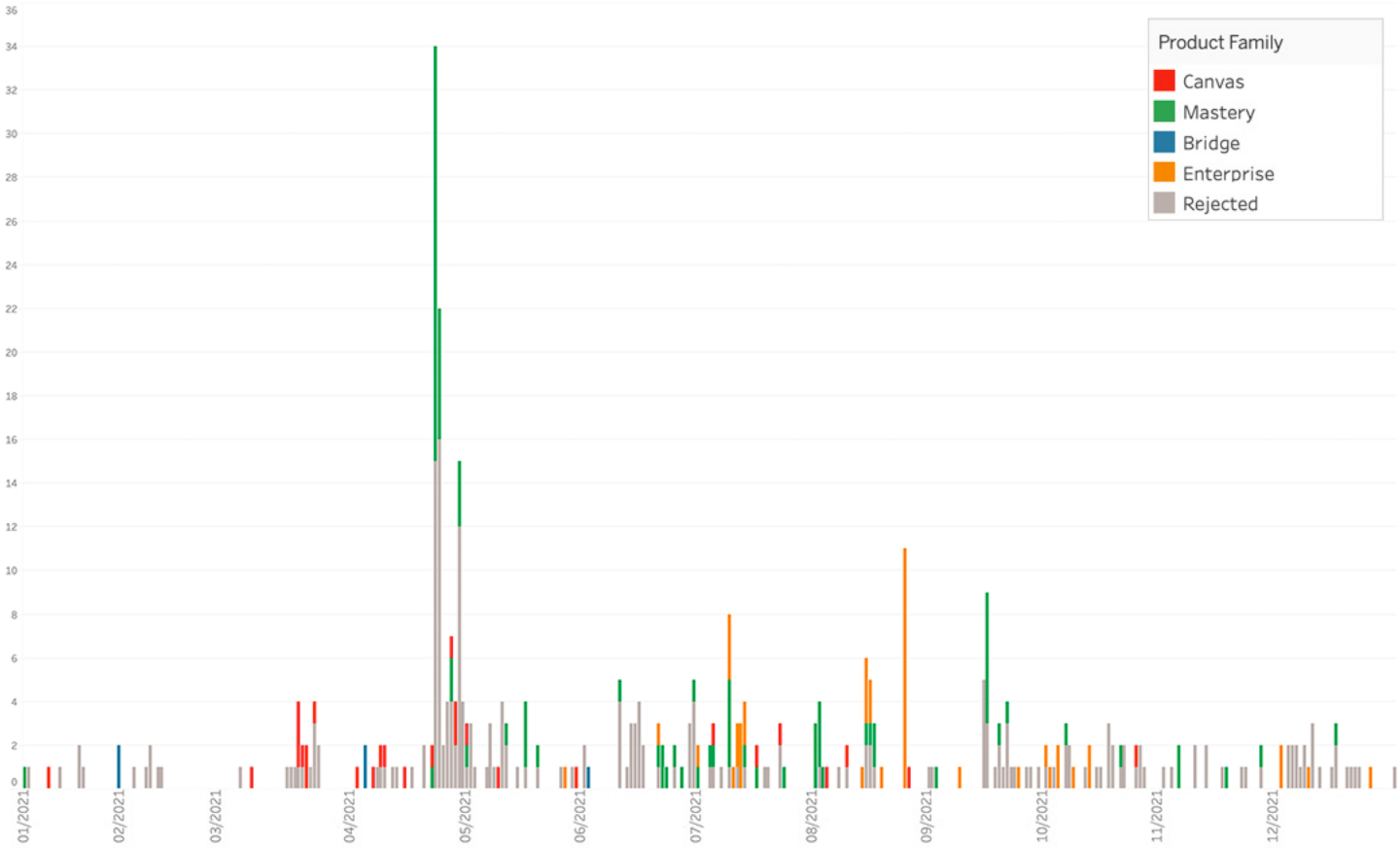
Findings by Product



Submissions over Time

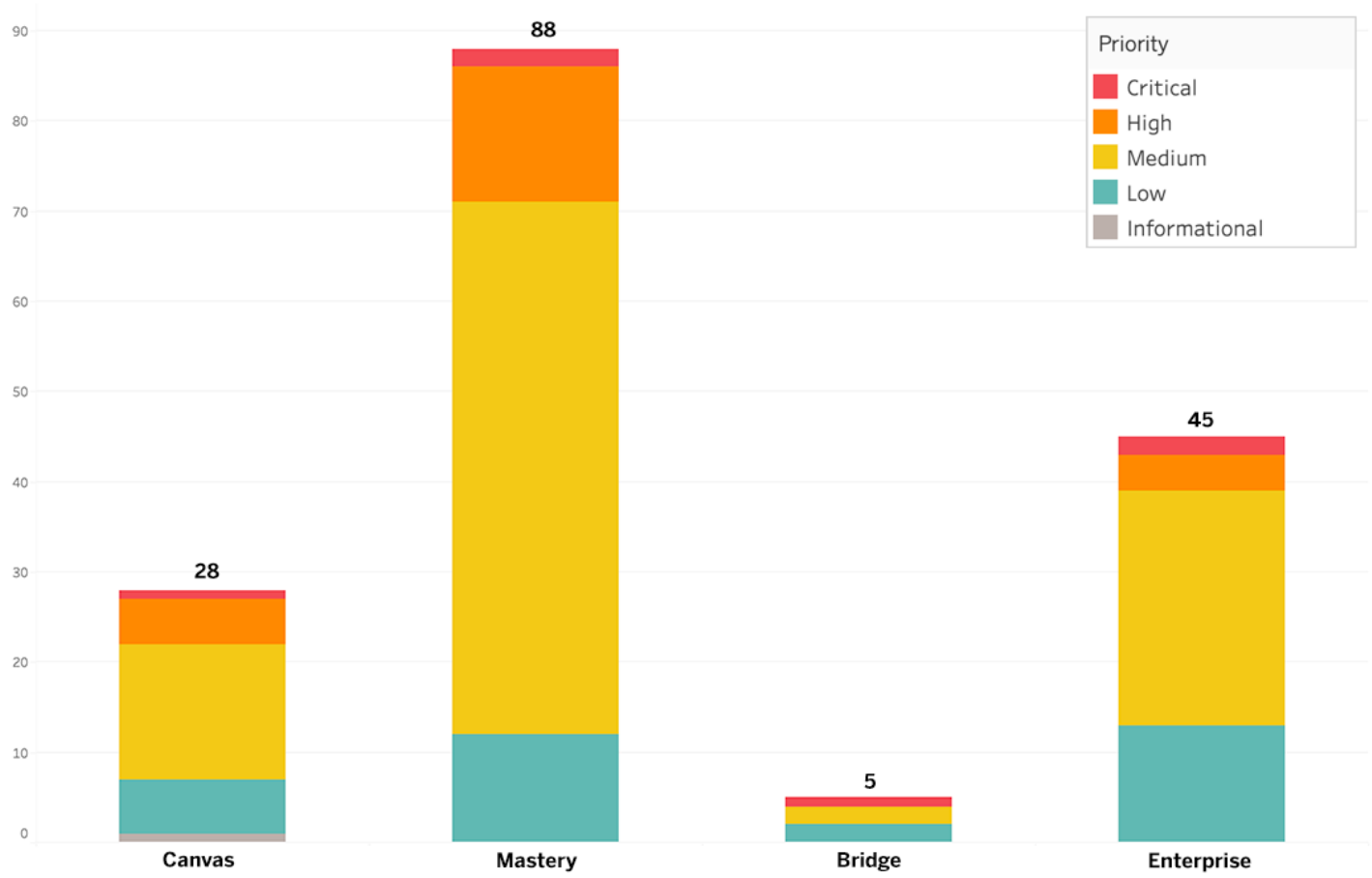
Included are auxiliary metrics and insights into the Ongoing program. This includes information regarding submissions over time, payouts and prevalent issue types.

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



Findings by Severity

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



Findings Table

Canvas

Canvas LMS (Web and API)

Our flagship learning environment that streamlines interaction and builds strong relationships between teachers and students, whether in the physical, blended or fully online classroom.

Title	VRT	Duplicates	Priority	State
RCE on .instructure.com	Server-Side Injection	0	Critical	Resolved
CSRF via Leakage of Token in POST to arbitrary site	Cross-Site Request Forgery (CSRF)	0	High	Resolved
No rate limit on adding Module leading to application level DOS because fetching all the added modules in single response via https://bugcrowd-tc.instructure.com/courses/16926/modules	Application-Level Denial-of-Service (DoS)	0	High	Resolved
Teacher [role] can access [Administrative data name, emails, PII] - [improper access control]	Broken Access Control (BAC)	0	High	Resolved
[postMessage] XSS in App registration	Cross-Site Scripting (XSS)	0	Medium	Resolved
Canvas does not verify POP3 server SSL certificate	Insecure Data Transport	0	Medium	Resolved
Open Redirect + Reflected XSS in iad.scorm.canvaslms.com - redirectonexiturl parameter	Cross-Site Scripting (XSS)	0	Medium	Resolved
Privileges Escalation (Student can submit the restricted submission type in assignment)	Broken Authentication and Session Management	0	Medium	Resolved
STEAL EMAILS and PHONE NUMBERS of ALL users in the same enrolled course	Sensitive Data Exposure	0	Medium	Resolved
Stored XSS as teacher via empty syllabus [bugcrowd-tc.instructure.com]	Cross-Site Scripting (XSS)	0	Medium	Resolved
Student can access chat even if it is disabled/hidden	Broken Authentication and Session Management	0	Medium	Resolved

Title	VRT	Duplicates	Priority	State
Student can access External Apps	Broken Authentication and Session Management	0	Medium	Resolved
Student can create group even if Instructor has restricted it	Broken Authentication and Session Management	1	Medium	Resolved
XSS in image with user-controlled src	Cross-Site Scripting (XSS)	0	Medium	Resolved
XSS via postMessage in Files	Cross-Site Scripting (XSS)	0	Medium	Resolved
[Stored] XSS as Student via observer feature	Cross-Site scripting (XSS)	0	Low	Resolved
No rate limit on rollcall email report	Server Security Misconfiguration	0	Low	Resolved
Privileges Escalation (student can submit quiz even if teacher locked it)	Broken Access Control (BAC)	0	Low	Resolved
Student can duplicate a teacher's discussion	Broken authentication and Session Management	0	Low	Resolved
Privileges Escalation {Submitting the student assessment after unpublish}	Broken authentication and Session Management	0	Informational	Resolved

Canvas Mobile (iOS and Android)

Title	VRT	Duplicates	Priority	State
Google Drive and Sheets API Service Misconfiguration allows an attacker to call APIs unauthorizedly. [Parent IOS And Student IOS APP]	Sensitive Data Exposure	0	Medium	Resolved
Newrelic Token Hardcoded in [Canvas Student Android Mobile APP]	Sensitive Data Exposure	1	Medium	Resolved

Canvas Studio

The next-generation video learning solution that turns one-way, passive video into inclusive, engaging, productive classroom discussions.

Instructure did not receive any valid Canvas Studio issues during the program period.

Canvas Student Pathways

Engages students through custom, stackable pathways, helps them navigate their academic and co-curricular journeys, and provides a roadmap for acquiring new skills.

Title	VRT	Duplicates	Priority	State
The integrity of google access token is not verified in qa.ops.portfolium.net	Server Security Misconfiguration	1	High	Resolved
Brute-Forcible login on dev4.edu.ops.portfolium.net	Server Security Misconfiguration	0	Low	Resolved
Bypass captcha verification on the forgot password page leads to mass mailing	Other	0	Low	Resolved

Canvas Commons

Title	VRT	Duplicates	Priority	State
XSS in https://commons-pdx-edge.inseng.net	Cross-Site Scripting (XSS)	0	High	Resolved
Student can "Share to Commons" an assignment	Broken Authentication and Session Management	0	Medium	Resolved

Canvas Catalog

Title	VRT	Duplicates	Priority	State
Canvas catalog allows bypass of email verification	Other	0	Medium	Resolved

Mastery

Mastery Connect (includes Web, API, and Android)

Our K–12 digital assessment management system that makes data-driven instruction a no-brainer and gives instant, visual views into student levels of understanding on any set of academic standards.

Title	VRT	Duplicates	Priority	State
IDOR: A school admin can leak temporary passwords of students of other district, can add himself as a parent of students and can lockout students accounts of other school/district	Broken Access Control (BAC)	0	Critical	Resolved
IDOR: I can leak password of students from other district + I can add myself as a parent to any student	Broken Access Control (BAC)	0	Critical	Resolved
Clone Report IDOR	Cross-Site Request Forgery (CSRF)	0	High	Resolved
CSRF the reset password leads to account take over	Cross-Site Request Forgery (CSRF)	0	High	Resolved
IDOR create new teacher leads to create Admin of any district, school	Broken Access Control (BAC)	3	High	Resolved
IDOR in parent account forget password which leads to 0 click account takeover of parents	Broken Access Control (BAC)	0	High	Resolved
IDOR: A school admin and A TEACHER can leak temporary passwords of students of other district and can add himself as a parent of students from any school/district	Broken Access Control (BAC)	0	High	Resolved
Privilege Escalation + IDOR in trackeredit endpoint which leads to temporary passwords of students of other district being leaked and attacker can add himself as a parent of students from any school/district	Broken Access Control (BAC)	0	High	Resolved
Stored XSS - Benchmark file upload [app.masteryconnect-security.com]	Cross-Site Scripting (XSS)	0	High	Resolved
stored xss in *Short Text* Item Bank	Cross-Site Scripting (XSS)	0	High	Resolved
stored xss in assessment *Title* field	Cross-Site Scripting (XSS)	2	High	Resolved
Stored XSS in Curriculum Maps Standard [app.masteryconnect-security.com]	Cross-Site Scripting (XSS)	17	High	Resolved
Stored XSS in Item Bank Passages [app.masteryconnect-security.com]	Cross-Site Scripting (XSS)	3	High	Resolved

Title	VRT	Duplicates	Priority	State
Stored XSS in Standard of Class Objective/Course	Cross-Site Scripting (XSS)	0	High	Resolved
Stored XSS On Grades Page	Cross-Site Scripting (XSS)	0	High	Resolved
View/Send Email Via https://app.masteryconnect-security.com/administration/students/email_student/1264648/administration/students/print_username	Broken Access Control (BAC)	3	High	Resolved
Wide app CSRF leads to District Administrator takeover [app.masteryconnect-security.com]	Cross-Site Request Forgery (CSRF)	6	High	Resolved
#2 IDOR On Classroom Archive	Broken Access Control (BAC)	0	Medium	Resolved
can use paid item from item bank by removing "disabled" attributes from source codes	Other	0	Medium	Resolved
Copy/Clone anyone's Curriculum Maps [app.masteryconnect-security.com]	Broken Authentication and Session Management	2	Medium	Resolved
CSRF in deleting tags [app.masteryconnect-security.com]	Cross-Site Request Forgery (CSRF)	0	Medium	Resolved
DOM XSS in 2 different fields in cloze math formula item bank	Cross-Site scripting (XSS)	2	Medium	Resolved
DOM XSS in cloze dropdown item bank	Cross-Site Scripting (XSS)	0	Medium	Resolved
IDOR - Add note to any Curriculum Map [app.masteryconnect-security.com]	Broken Access Control (BAC)	1	Medium	Resolved
IDOR - Print anyone's Curriculum Maps [app.masteryconnect-security.com]	Broken Access Control (BAC)	0	Medium	Resolved
IDOR - Remove a Standard in any Curriculum Map	Broken Access Control (BAC)	0	Medium	Resolved
IDOR "Bypass"	Broken Access Control (BAC)	0	Medium	Resolved
IDOR Can reply to message thread of other user [app.masteryconnect-security.com]	Broken Access Control (BAC)	3	Medium	Resolved
IDOR Delete Section [gradebook.masteryconnect-security.com]	Broken Access Control (BAC)	0	Medium	Resolved

Title	VRT	Duplicates	Priority	State
IDOR Edit team data of other users [app.masteryconnect-security.com]	Broken Access Control (BAC)	5	Medium	Resolved
IDOR leads to manage curriculum_maps feature of other district [app.masteryconnect-security.com]	Broken Access Control (BAC)	11	Medium	Resolved
IDOR On CMAP	Broken Access Control (BAC)	0	Medium	Resolved
IDOR on Delete Section[app.masteryconnect-security.com]	Broken Access Control (BAC)	1	Medium	Resolved
IDOR on edit section [gradebook.masteryconnect-security.com]	Broken Access Control (BAC)	0	Medium	Resolved
IDOR on edit section[app.masteryconnect-security.com]	Broken Access Control (BAC)	2	Medium	Resolved
IDOR on Editing Report Assessment	Broken Access Control (BAC)	1	Medium	Resolved
IDOR teacher can manager the student of other school, district [app.masteryconnect-security.com]	Broken Access Control (BAC)	0	Medium	Resolved
IDOR the notification id value leads to can comment to private user	Broken Access Control (BAC)	0	Medium	Resolved
IDOR to Archive the admin's CMAP	Broken Access Control (BAC)	0	Medium	Resolved
IDOR to delete custom report - /reports/edit_custom_report [app.masteryconnect-security.com]	Broken Access Control (BAC)	2	Medium	Resolved
IDOR to Edit the Launch grader answer	Broken Access Control (BAC)	0	Medium	Resolved
IDOR to edit victim's student score	Broken Access Control (BAC)	0	Medium	Resolved
IDOR To export student data and tracker to xls file	Broken Access Control (BAC)	0	Medium	Resolved
IDOR to Mark the visibility of classroom	Broken Access Control (BAC)	0	Medium	Resolved
IDOR Use someone's "private" Standard in your Curriculum Map	Broken Access Control (BAC)	1	Medium	Resolved
IDOR View Other Custom Report	Broken Access Control (BAC)	0	Medium	Resolved
IDOR: Accessing private Assessments of other users at [https://app.masteryconnect-security.com/choose/ID-Here]	Broken Access Control (BAC)	0	Medium	Resolved

Title	VRT	Duplicates	Priority	State
IDOR: Accessing private MAPs of other users	Broken Access Control (BAC)	0	Medium	Resolved
IDOR: Adding undeletable map to any user + Missing rate limit which leads to adding 100s of maps to any users account	Broken Access Control (BAC)	0	Medium	Resolved
IDOR: I Can add my section to any school/district	Broken Access Control (BAC)	0	Medium	Resolved
IDOR: I can add my students to anyone trackers can can access its data	Broken Access Control (BAC)	0	Medium	Resolved
IDOR: I can add students to other districts	Broken Access Control (BAC)	0	Medium	Resolved
IDOR: I can comment on anyone private assessment at [https://app.masteryconnect-security.com/materials/530762/comments] + missing rate limit on comment endpoint	Broken Access Control (BAC)	0	Medium	Resolved
IDOR: I can delete any student from any tracker	Broken Access Control (BAC)	0	Medium	Resolved
IDOR: I can delete student from any classroom at https://gradebook.masteryconnect-security.com/classrooms]	Broken Access Control (BAC)	0	Medium	Resolved
IDOR: I can see private map of other user via archive feature	Broken Access Control (BAC)	0	Medium	Resolved
IDOR: I can see private standard of any user + I can add my own pins to other users boards	Broken Access Control (BAC)	0	Medium	Resolved
IDOR: One parent can see the other parents and students notes	Broken Access Control (BAC)	0	Medium	Resolved
IDOR: Privilege Escalation from school admin to District admin	Broken Access Control (BAC)	0	Medium	Resolved
Modify other parent accounts	Broken Access Control (BAC)	1	Medium	Resolved
Privilege Escalation: A Instructional Coach can add a new student by forced Browsing [accessing adding new student endpoint directly]	Broken Authentication and Session Management	0	Medium	Resolved
Stored XSS - CSV downloads	Cross-Site Scripting (XSS)	0	Medium	Resolved
Stored XSS - Item banks	Cross-Site scripting (XSS)	0	Medium	Resolved

Title	VRT	Duplicates	Priority	State
Stored xss at Sub Standard (tracker module)	Cross-Site Scripting (XSS)	1	Medium	Resolved
Stored XSS at unit name [app.masteryconnect-security.com]	Cross-Site Scripting (XSS)	1	Medium	Resolved
stored xss in *Number line plot* item bank at [https://app.masteryconnect-security.com/administration/item_banks/*id*]	Cross-Site scripting (XSS)	0	Medium	Resolved
Stored xss in *Student Number* from school admin to District admin	Cross-Site scripting (XSS)	1	Medium	Resolved
Stored XSS in /curriculum_maps/{id}/note	Cross-Site Scripting (XSS)	4	Medium	Resolved
Stored xss in class name	Cross-Site Scripting (XSS)	1	Medium	Resolved
Stored XSS in file name while uploading it	Cross-Site scripting (XSS)	0	Medium	Resolved
Stored xss in order list item bank from school admin to district admin	Cross-Site Scripting (XSS)	0	Medium	Resolved
Stored XSS in Tags [app.masteryconnect-security.com]	Cross-Site Scripting (XSS)	6	Medium	Resolved
STORED XSS Within Curriculum Map Standards AGAIN!!	Cross-Site Scripting (XSS)	0	Medium	Resolved
Teacher can edit, clone and archive other teacher's progress report	Broken Access Control (BAC)	0	Medium	Resolved
View Unit of a private Curriculum Map | https://app.masteryconnect-security.com/curriculum_maps//units//add_document	Broken Access Control (BAC)	0	Medium	Resolved
#2 IDOR to Mark the Display of classroom	Broken Access Control (BAC)	0	Low	Resolved
#3 No rate IImit on Email student report	Server Security Misconfiguration	0	Low	Resolved
#4 No rate Limit on teacher inbox email	Server Security Misconfiguration	0	Low	Resolved
Comment can be created on assessment which has been made private [app.masteryconnect-security.com]	Broken authentication and Session Management	1	Low	Resolved
IDOR - Set a power standard to any Curriculum Map	Broken Access Control (BAC)	0	Low	Resolved

Title	VRT	Duplicates	Priority	State
IDOR on downloading report	Broken Access Control (BAC)	2	Low	Resolved
No rate limit email triggering - setup/invite [app.masteryconnect-security.com]	Server Security Misconfiguration	0	Low	Resolved
No rate limit on registration leads to mass registrations	Server Security Misconfiguration	0	Low	Resolved
No rate limiting VIa Send Student Invitation https://app.masteryconnect-security.com/administration/students	Server Security Misconfiguration	0	Low	Resolved
No rate limiting Via Send Teacher Invitation Via https://app.masteryconnect-security.com/administration/teachers/252934/send-activation	Server Security Misconfiguration	0	Low	Resolved
Open Redirect - redirect_uri parameter	Unvalidated Redirects and Forwards	2	Low	Resolved
Stored XSS - Progress Reports	Cross-Site scripting (XSS)	0	Low	Resolved

Bridge (legacy)

A learning platform for all things performance, that helps employees and managers transform their organization through connection, alignment, and growth.

Bridge Suite

Title	VRT	Duplicates	Priority	State
CVE-2019–5418 - LFI of system and application files	Server-Side Injection	0	Critical	Resolved
User with learner permission is able to delete account_admin tasks	Broken Access Control (BAC)	0	Medium	Resolved

Practice

Title	VRT	Duplicates	Priority	State
A user with learner role access is able to fetch invited customers details of other organisations (email, name, Organisation ID, Organisation Names) - PII Disclosure - Improper Access control	Other	0	Medium	Resolved
No rate limit on creating Content Modules via /organizations/1053030/content-modules, leading to application level DOS because fetching all the added Modules in single response.	Application-Level Denial-of-Service (DoS)	0	Low	Resolved
No rate limit on creating Groups via /organizations/1053030/groups, leading to application level DOS because fetching all the added groups in single response.	Application-Level Denial-of-Service (DoS)	0	Low	Resolved

Enterprise

Included in the Bugcrowd security program is enterprise testing of our own security program, platforms, and infrastructure.

DNS

Title	VRT	Duplicates	Priority	State
Domain Takeover Via Oracle on *.higheredsoftware.com	Server Security Misconfiguration	0	High	Resolved
Subdomain Takeover Via Dangling NS records pointed to Amazon EC2 elastic Ips at http://bouncer3.us-east-1.cisco-staging.insops.net	Server Security Misconfiguration	0	High	Resolved
Subdomain Takeover Via Unclaimed aws s3 bucket for training.netacadadvantage.com/index2.html	Server Security Misconfiguration	0	High	Resolved
Subdomain Takeover Via Unclaimed Azure Website 0d4f1f5abc.docs.dataconnectdev.certicaconnect.com	Server Security Misconfiguration	0	Medium	Resolved
Hosted Zone Takeover of instructure.com.au via DNS Made Easy Secondary DNS	Server Security Misconfiguration	0	Medium	Resolved
Hosted Zone Takeover of instructure.uk via DNS Made Easy Secondary DNS	Server Security Misconfiguration	0	Medium	Resolved
Subdomain Takeover at code42.instructure.com	Server Security Misconfiguration	0	Medium	Resolved

Title	VRT	Duplicates	Priority	State
Subdomain takeover of api-testmindful.masteryconnect.com	Server Security Misconfiguration	0	Medium	Resolved
Subdomain takeover of blog-test.masteryconnect.com	Server Security Misconfiguration	0	Medium	Resolved
Subdomain takeover of bridgesupport.inseng.net	Server Security Misconfiguration	0	Medium	Resolved
Subdomain takeover of c2d2.inssec.info	Server Security Misconfiguration	0	Medium	Resolved
Subdomain takeover of hris.inseng.net	Server Security Misconfiguration	0	Medium	Resolved
Subdomain takeover of mailcatcher.inseng.net	Server Security Misconfiguration	0	Medium	Resolved
Subdomain takeover of minecraft.inseng.net	Server Security Misconfiguration	0	Medium	Resolved
Subdomain takeover of postgresql.ax.instructure.com	Server Security Misconfiguration	0	Medium	Resolved
Subdomain takeover of puppet-test.instructure.com	Server Security Misconfiguration	0	Medium	Resolved
Subdomain takeover of troll-prod-web-235892251.inseng.net	Server Security Misconfiguration	0	Medium	Resolved
Subdomain takeover of upgrade.masteryconnect.com	Server Security Misconfiguration	0	Medium	Resolved
Subdomain Takeover Via Dangling NS records pointed to Amazon EC2 elastic Ips at http://jump1.us-east-1.test.insops.net	Server Security Misconfiguration	0	Medium	Resolved
Subdomain Takeover Via Dangling NS records pointed to Amazon EC2 elastic Ips at http://teamcity.certicasolutions.com	Server Security Misconfiguration	0	Medium	Resolved
Subdomain Takeover Via Unclaimed Acquia.com domain for ondeck.arcmedia.com	Server Security Misconfiguration	0	Medium	Resolved
Subdomain Takeover Via Unclaimed Acquia.com domain for ondeckdev.blog.canvaslms.com	Server Security Misconfiguration	0	Medium	Resolved
Subdomain Takeover Via Unclaimed Azure Website 0d4f1f5abc.admin.dataconnectdev.certicaconnect.com	Server Security Misconfiguration	0	Medium	Resolved
Subdomain Takeover Via Unclaimed Azure Website 0d4f1f5abc.docs.sandbox.dataconnectdev.certicaconnect.com	Server Security Misconfiguration	0	Medium	Resolved

Title	VRT	Duplicates	Priority	State
Subdomain Takeover Via Unclaimed Azure Website 0d4f1f5abc.odsapi.dataconnectdev.certicaconnect.com	Server Security Misconfiguration	0	Medium	Resolved
Subdomain Takeover Via Unclaimed Azure Website 0d4f1f5abc.odsapi.sandbox.dataconnectdev.certicaconnect.com	Server Security Misconfiguration	0	Medium	Resolved
Subdomain Takeover Via Unclaimed Azure Website 0d4f1f5abc.v2bridge.dataconnectdev.certicaconnect.com	Server Security Misconfiguration	0	Medium	Resolved
Subdomain Takeover Via Unclaimed Azure Website 0d4f1f5abc.v2bridge.sandbox.dataconnectdev.certicaconnect.com	Server Security Misconfiguration	0	Medium	Resolved
Hosted Zone Takeover of canvas-lms.com via Rackspace Cloud DNS	Server Security Misconfiguration	0	Low	Resolved
Hosted Zone Takeover of canvas-lms.org via Rackspace Cloud DNS	Server Security Misconfiguration	0	Low	Resolved
Hosted Zone Takeover of canvasinstructure.com via Rackspace Cloud DNS	Server Security Misconfiguration	0	Low	Resolved
Hosted Zone Takeover of canvasinstructure.org via Rackspace Cloud DNS	Server Security Misconfiguration	0	Low	Resolved
Hosted Zone Takeover of canvaslms.org via Rackspace Cloud	Server Security Misconfiguration	0	Low	Resolved
Hosted Zone Takeover of canvassucks.com via Rackspace Cloud DNS	Server Security Misconfiguration	0	Low	Resolved
Hosted Zone Takeover of canvassucks.org via Rackspace Cloud DNS	Server Security Misconfiguration	0	Low	Resolved
Hosted Zone Takeover of instructurecanvas.com via Rackspace Cloud DNS	Server Security Misconfiguration	0	Low	Resolved
Hosted Zone Takeover of instructurecanvas.org via Rackspace Cloud DNS	Server Security Misconfiguration	0	Low	Resolved
Hosted Zone Takeover of instructurelms.com via Rackspace Cloud	Server Security Misconfiguration	0	Low	Resolved
Hosted Zone Takeover of instructurelms.org via Rackspace Cloud DNS	Server Security Misconfiguration	0	Low	Resolved

Other

Service	Title	VRT	Duplicates	Priority	State
Discourse	Remote Code Execution on Discourse via CVE-2021-41163	Server-Side Injection	0	Critical	Resolved
Tableau	Remote Code Execution on Tableau	Server-Side Injection	0	Critical	Resolved
JIRA Service Desk	Accidental Access to a canvas admin account	Other	0	High	Resolved
Google Forms	Publicly accessible resource exposes PII info via google	Sensitive Data Exposure	0	Low	Resolved
JIRA Service Desk	Open redirect on https://gw.masteryconnect.com	Unvalidated Redirects and Forwards	0	Low	Resolved

Appendix

Spend of Program Rewards Pool

During this Ongoing program, about **26%** of the total allocated reward pool of **$264,375 USD** was paid. A number of other statistics regarding the Ongoing Program's payouts are shown below.

$68,900.00 total paid out to researchers	**$69,650.00** total to be paid to researchers	**$39,900.00** remaining prize pool
$1,000. highest paid reward	**$50.00** lowest paid reward	**$304.87** average reward

Top 3 Highest Paid Submissions

Vulnerability	Reward
Remote Code Execution on [anyinstance].instructure.com	$1,500.00 USD
Remote Code Execution at on Discourse via CVE-2021-41163	$1,500.00 USD
Remote Code Execution on Tableau due to CVE-2021-44228	$1,500.00 USD