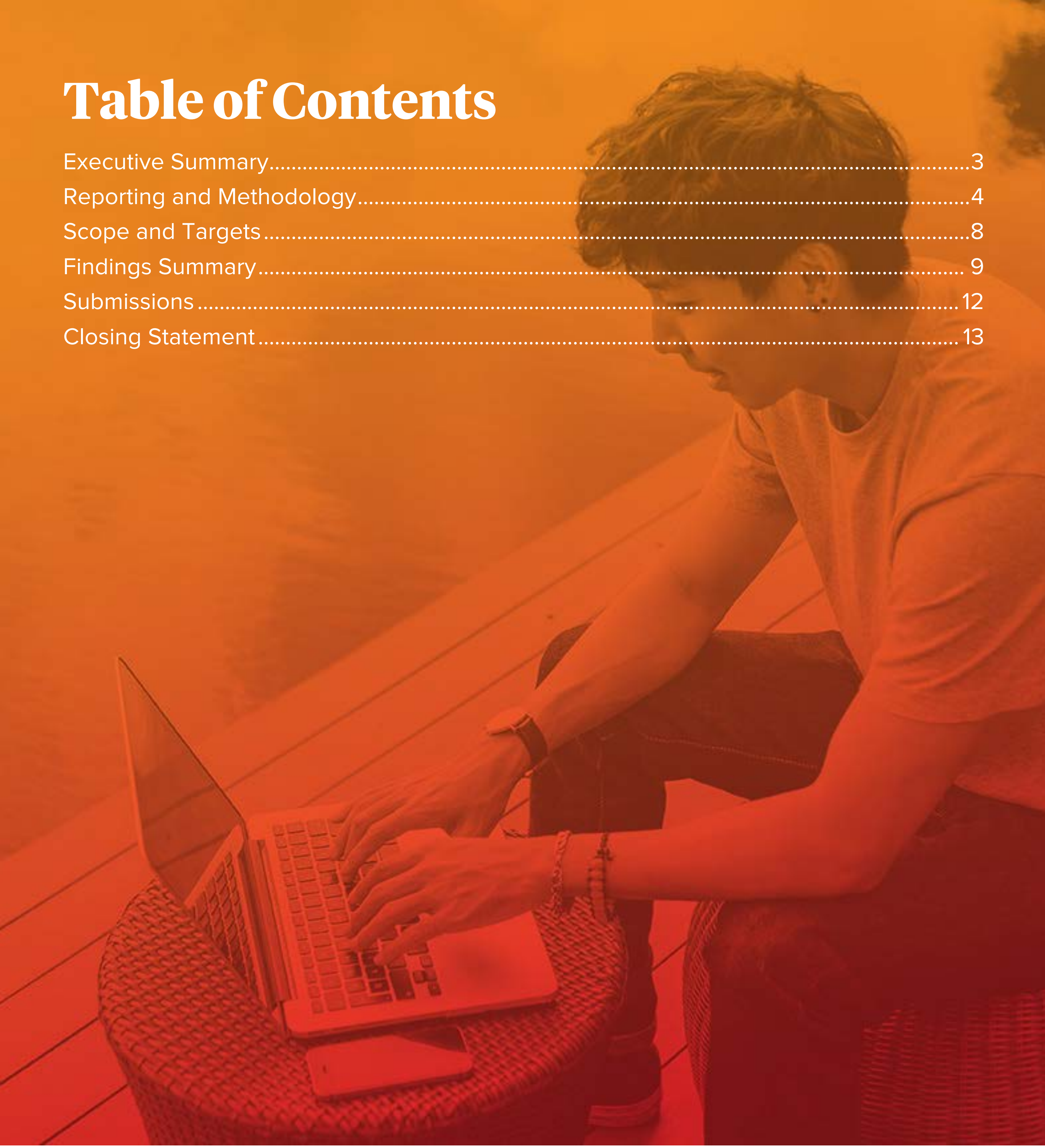
CANVAS
BY INSTRUCTURE

# SECURITY AUDIT REPORT

Canvas LMS, Studio, and Catalog

April 2023

# Table of Contents



# Executive Summary

Dear customers,

I am pleased to present the Canvas annual security audit report. As our product family continues to grow and the Instructure Learning Platform becomes a complete end to end platform for our customers, this year, we made the decision to split our Security Audit Report by product. Once again, Instructure has engaged Bugcrowd, Inc. to host our private bug bounty program, and **I am pleased to announce that all issues listed within this report are resolved.** 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 audits available to customers, both publicly on our website and directly when requested.

The purpose of our Ongoing Bounty Program and penetration testing is to identify security vulnerabilities that may threaten both our, and our customers, security. Once identified, each vulnerability is rated for technical impact defined in the findings summary section of the report.

This report shows testing for Canvas LMS, Canvas Studio, and Canvas Catalog. It covers the full 2022 year during the period of **January 1st 2022 through December 31st 2022.** During this period, **10** valid Canvas product submissions were accepted from a pool total of **37** 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

## 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 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 shortened test periods.

To further help get Bugcrowd security researchers started, we provide the Canvas LMS source code (https://github.com/instructure/canvas-lms) with a goal of transparency in the hope it assists in revealing potential issues in our code base that may help a researcher find vulnerabilities in our live application. By reviewing the source code, a security researcher can gain a much deeper understanding of where vulnerabilities may be, and perhaps an easier time exploiting those issues for reward. Naturally, since this is source code, some findings may not be exploitable due to the many other protections we have in place.

## Ongoing Program Methodology

It is important to note that this report 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.

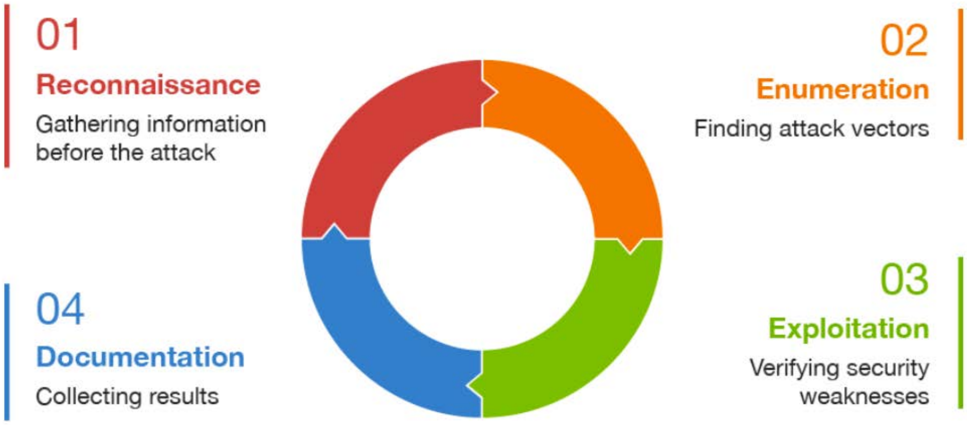
## Testing Methods

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.

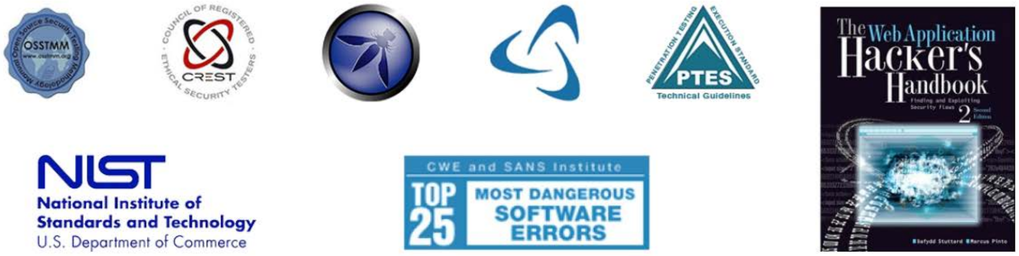
## Background

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 the Bugcrowd Ongoing Program.

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:


OSSTMM
Open Source Security Testing Methodology Manual
www.osstmm.org
COUNCIL OF REGISTERED ETHICAL SECURITY TESTERS
CREST
PENETRATION TESTING EXECUTION STANDARD
PTES
Technical Guidelines
The Web Application Hacker's Handbook
Finding and Exploiting Security Flaws
2 Second Edition
Dafydd Stuttard Marcus Pinto
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
CWE and SANS Institute
TOP 25
MOST DANGEROUS SOFTWARE ERRORS

# 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**<br>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<br>• Vertical Authentication Bypass<br>• XML External Entities Injection<br>• SQL Injection<br>• Insecure Direct Object Reference for a critical function |
| **High**<br>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<br>• Stored Cross-Site Scripting<br>• Cross-Site Request Forgery for a critical function<br>• Insecure Direct Object Reference for an important function<br>• Internal Server-Side Request Forgery |

| | |
|---|---|
| **Medium**<br>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<br>• Cross-Site Request Forgery for an important function<br>• Insecure Direct Object Reference for an unimportant function |
| **Low**<br>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<br>• Cross-Site Request Forgery for an unimportant function<br>• External Server-Side Request Forgery |
| **Informational**<br>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<br>• Autocomplete enabled<br>• Non-exploitable SSL issues |

VRT

**Bugcrowd's Vulnerability Rating Taxonomy**

More detailed information regarding our vulnerability classification can be found at:

https://bugcrowd.com/vrt

# Scope and Targets

## Scope

Bugcrowd works with Instructure to define the Rules of Engagement, commonly known as the program brief, which includes the scope of work. For our Canvas Security Audit, the following targets were considered explicitly in scope for testing:

## Targets

### Canvas LMS

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

### Canvas Mobile Applications

`Canvas Student`

`Canvas Teacher`

`Canvas Parent`

### Canvas Commons

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

### Canvas Catalog

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

### Canvas Studio

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

# Findings Summary

## Summary

During the program, Bugcrowd researchers discovered the following counts for the Canvas product family:

| Priority | Canvas LMS^ | Studio | Catalog | Total |
|---|---:|---:|---:|---:|
| Critical (P1) | 2 | 0 | 0 | 2 |
| High (P2) | 1 | 0 | 0 | 1 |
| Medium (P3) | 6 | 0 | 0 | 6 |
| Low (P4) | 1 | 0 | 0 | 1 |
| Informational* | 16 | 0 | 0 | 16 |
| **Canvas Product Family Total** | | | | **26** |

^Includes Canvas LMS, Mobile Applications, and Canvas Commons

*Informational are those issues submitted but not counted as issues, either because they are not security issues and/or do not pose any threats.

# Vulnerabilities

## 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 | Priority | State |
|---|---|---|---|
| [www.canvaslms.com] AWS keys leakage from Apache SSRF (CVE-2021-40438) via proxy pass on /core/misc/ | Broken Access Control (BAC) | 1 | RESOLVED |
| SQL injection in /api/lti/accounts/$id/jwt_token | Server-Side Injection | 1 | RESOLVED |
| [Stored XSS] on rich text editors generated code (via "area" html tag) | Cross-Site Scripting (XSS) | 2 | RESOLVED |
| Subdomain takeover at ondeck.canvaslms.com | Server Security Misconfiguration | 3 | RESOLVED |
| Subdomain takeover of jobs1-bouncer.us-east-1c.canvas.insops.net | Server Security Misconfiguration | 3 | RESOLVED |
| Subdomain Takeover at auckland-roster-test.canvaslms.com | Server Security Misconfiguration | 3 | RESOLVED |
| DOM XSS - api.eu-west-1.instructure.com | Cross-Site Scripting (XSS) | 3 | RESOLVED |
| [tip.instructure.com] DOM XSS via arbitrary script loading | Cross-Site Scripting (XSS) | 3 | RESOLVED |
| partial CSRF allowing changing grades and possible other sensitive actions | Cross-Site Request Forgery (CSRF) | 3 | RESOLVED |

## Canvas Mobile (iOS and Android)

| Title | VRT | Priority | State |
|---|---|---|---|
| A vulnerability in com.instructure.android (Canvas Student) allows an attacker to exploit an intent returned by DocumentScanningActivity to access users personal info (name, email and personal scanned/uploaded documents) | Broken Authentication and Session Management | 4 | 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.

## Commons

Canvas Commons is a learning object repository that enables educators to find, import, and share resources.

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

## Catalog

Canvas Catalog is an elegant, all-in-one learning solution that includes a course catalog customized to your institution, course registration system, payment gateway, and learning platform.

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

# Submissions

## Signal to Noise

For 2022, a total of **26** submissions were received across all Canvas products, with **10** unique valid issues discovered. Bugcrowd identified **16** informational submissions and **6** duplicate submissions. The ratio of unique, valid submissions to noise was **46%**.

| Submission Outcome | Canvas LMS^ | Studio | Catalog | Total |
|---|---|---|---|---|
| Valid | 10 | 0 | 0 | **10** |
| Invalid | 16 | 0 | 0 | **16** |
| Duplicates | 6 | 0 | 0 | **6** |

## Program Rewards

During 2022, **11** rewards were paid out of Instructure's total allocated reward pool towards validated vulnerabilities in Canvas Product Family products.

## Top 3 highest paid Canvas submissions

| Vulnerability | VRT |
|---|---|
| [www.canvaslms.com] AWS keys leakage from Apache SSRF (CVE-2021-40438) via proxy pass on /core/misc/ | Broken Access Control (BAC) |
| SQL injection in /api/lti/accounts/$id/jwt_token | Server-Side Injection |
| [Stored XSS] on rich text editors generated code (via "area" html tag) | Cross-Site Scripting (XSS) |

# Closing Statement

## Year in Review

The security landscape is constantly changing, and at Instructure, we are committed to meeting this changing landscape with a dedicated, highly skilled, in-house security team improving the security of our products and services on an ongoing basis. No technology company is immune to security threats. That’s why when it comes to protecting our customers, the industry as a whole needs to work together to identify best security practices. As we continue to enhance our security capabilities across all stages of our software development lifecycle, we welcome participation from all members of the community–our customers, employees, security researchers, and valued partners. Some could say we view security as a ‘team sport’, and we encourage you to keep us informed in making our platform more secure. Naturally, like any technology organization committed to security, we have our own plans we’re working on to improve our defenses against badness and developments that might negatively impact your learning experience using our products. While we do many things well, we are always finding ways we can improve.

Alongside plans to incorporate third-party security assessments into our capabilities, we want to further enhance our bug bounty program and take it to the next level. We find Bugcrowd’s service to be extremely valuable and have found that no other provider has been able to match the level of support in this area.

In today's hyper-speed world, standalone penetration testing simply isn't sufficient to counter opportunistic bad actors who don't adhere to any predefined schedule. In engaging Bugcrowd to supplement our internal practices with an ongoing bug bounty program, Instructure can remediate discovered vulnerabilities before threat actors can exploit them–*year-round*–through a highly talented pool of security researchers and a platform that helps us triage and respond faster.

Lastly, we extend an invitation to all security researchers to join our bug bounty program, where we pay rewards for validated findings. If you are interested in joining, please send your Bugcrowd ID to security@instructure.com.

This is another way we demonstrate our commitment to taking the security of your data seriously.

Keep Learning.

INSTRUCTURE