bugcrowd

Instructure Canvas Web Application
Bugcrowd On-Demand Program Retest Results
April 6, 2017

Executive Summary

Instructure engaged Bugcrowd Inc to perform an On-Demand Bounty Program – commonly known as a crowd-sourced penetration test – on **Instructure's Canvas Web Application**. Testing occurred during the period: **01/31/2017** – **02/14/2017**.

For this On-Demand program, **50** researchers were invited to participate; **45** accepted the invitation, resulting in **51** vulnerability submissions received from **17** unique researchers. These issues ranged in scope and severity, with **1** critical priority **P1** issue(s) discovered. As a whole, researchers with rewardable submissions received **$15,000** out of a total prize pool of **$15,000**.

This report is just a summary of the information available. You can find all details – including vulnerability remediation – of your program in the Bugcrowd Crowdcontrol Tracker: https://tracker.bugcrowd.com. If you have any questions or comments, please contact support@bugcrowd.com.

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, we encourage researchers to use their own individual methodologies when participating in Bugcrowd On-Demand programs.

The workflow of every penetration test can be divided into four phases: **reconnaissance, enumeration**, **exploitation** and **documentation**.

- **Reconnaissance:**
Gathering information before the attack

- **Enumeration:**
Finding attack vectors

- **Exploitation:**
Verifying security weaknesses

- **Documentation:**
Collecting results

Bugcrowd researchers who perform web application testing and vulnerability assessment usually subscribe to a variety of methodologies following this workflow, including: the **OWASP 4.0 Testing Guide**, the **Penetration Testers Execution Standard**, and the **WAHH Methodology**.

Targets

Similar to a regular penetration test, an On-Demand program defines Rules of Engagement in the Bounty Brief or Scope. For this On-Demand program, the following targets were considered in-scope for testing:

- `bugcrowd-tc.instructure.com`
- `*.test.instructuremedia.com`

Priority Key

The following priority matrix is used as a guideline to classify valid assessment findings:

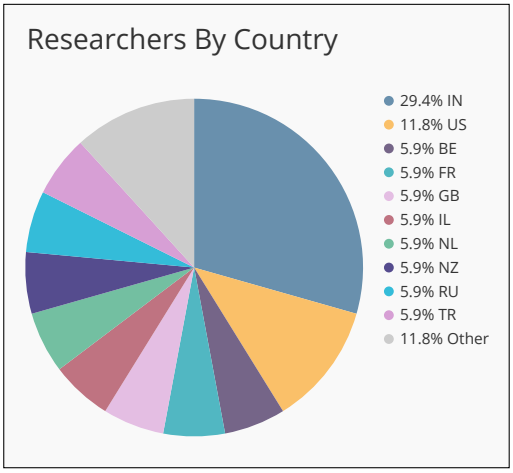
Priority	Impact	Example Vulnerability Types
P1 – Critical	Vulnerabilities that cause a privilege escalation from unprivileged to admin or allow for remote execution, financial theft, etc.	• Remote Code Execution • Vertical Authentication Bypass • XML External Entities Injection • SQL Injection • Insecure Direct Object Reference for a critical function
P2 – High	Vulnerabilities that affect the security of the platform including the processes it supports	• Lateral authentication bypass • Stored Cross-Site Scripting • Cross-Site Request Forgery for a critical function • Insecure Direct Object Reference for an important funtion • Internal Server-Side Request Forgery
P3 – Medium	Vulnerabilities that affect multiple users and require little or no user interaction to trigger	• Reflected Cross-Site Scripting with limited impact • Cross-Site Request Forgery for an important fuction • Insecure Direct Object Reference for an unimportant fuction • URL redirect
P4 – Low	Vulnerabilities that affect singular users and require interaction or significant prerequisites to trigger (MitM) to trigger	• Cross-Site Scripting with limited impact • Cross-Site Request Forgery for an unimportant function • External Server-Side Request Forgery

Bugcrowd's Vulnerability Taxonomy

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

On-Demand Bounty Program Overview

An On-Demand program is a novel approach to an application assessment or penetration test. Traditional penetration tests use only one or two researchers to test an entire application, while On-Demand programs leverage 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.



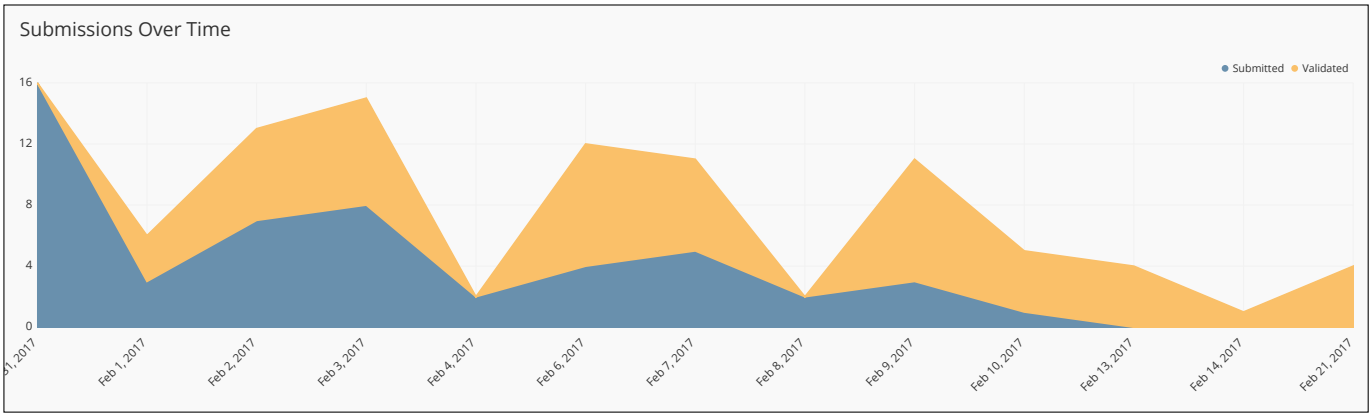
The On-Demand program for **Instructure's Canvas Web Application** received submissions from **17** researchers in the following countries: **Belgium, France, India, Israel, the Netherlands, New Zealand, Russia, Turkey, Ukraine, the United Kingdom, the United States, and Vietnam**. Most of the researchers are based in **India**.

Submissions Count

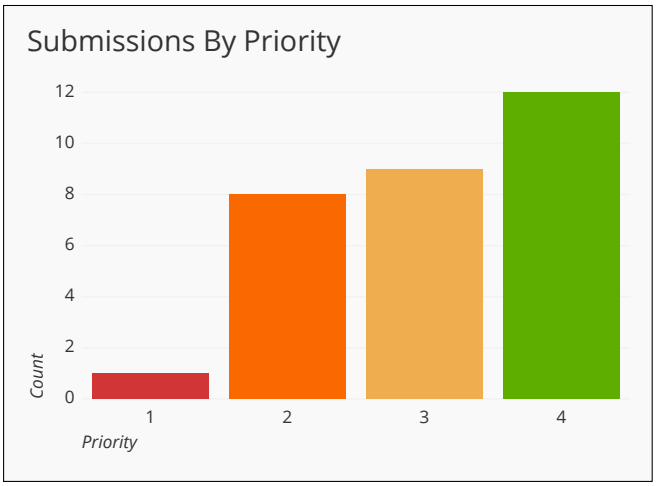
Outcome	count
Valid	30
Duplicate	5
Wont Fix	11
Invalid	5
Total	51

A total of **51** submissions were received, with **30** unique valid issues discovered. Bugcrowd identified **5** duplicate and **11** won't fix submission(s), and removed **5** invalid submission(s).

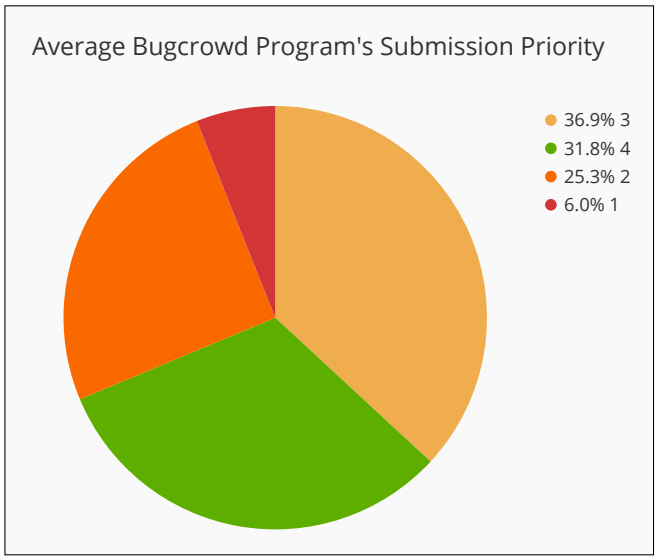
The timeline below shows submissions received and validated by the Bugcrowd team:

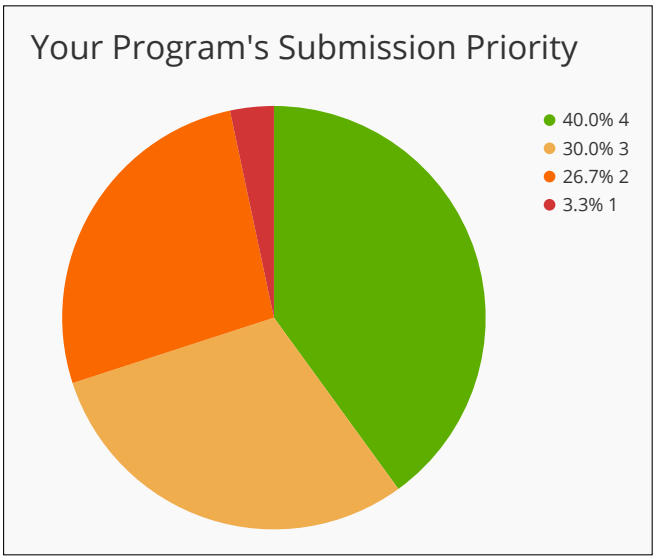


Bugcrowd ranks the technical priority of all confirmed findings on a scale from P1 (Critical) to P4 (Low). The results are shown to the right. The majority of submissions to the **Instructure Canvas Web Application** On-Demand program were **P4**.



A comparison of submissions by priority for Bugcrowd's other On-Demand programs to that of the **Instructure Canvas Web Application** On-Demand program is shown below.





All Valid Submissions

Title	Reference Number	Priority	Reward	Retest
XML External Entity Expansion Through Import Content Yields Arbitrary File Read Access on Server	15499bf78005b246596331ba70f61d8de58147ecaab6c5a21ce0a094fde54769	1	$1,737.93	Resolved
Error_controller is vulnerable to stored XSS via url parameter	53f119b8203956c7c99d35416c96216034af50d0136b43cf1af341bb6b61f2b8	2	$868.96	**Unresolved**
GZIP bomb DoS on /login/saml/logout via SAMLRequest	e0e44866a2a4c981ff4bab5ff722bf164ea514664104ee1e55380d73f7b16a8b	2	$868.96	Resolved
Stored XSS in Quizzes through uploaded QTI file	721aa087562a7e21c10a75b4bd3e57204ad4e59fcc41869c00628b4411922c58	2	$868.96	Resolved
Stored XSS on /api/v1/courses/113/external_tool via external_tool(url)	f927e83dbf38fc1c9a1c9860912104082450fbe11b0d5a9d0c7de75d315ab2ba	2	$868.96	Resolved
Stored XSS on every page with rich text editor	d2164e51825f95e4f31be56ad7c24544a992c068fef628f2a608dace7a7f45cf	2	$868.96	Resolved
Stored XSS using caption file	6084694504674a6ad19b800cd3d1ae76f126cba9eeb7e35c3e39407bf3c5bd3e	2	$868.96	Resolved
View any page when knowing the url - `https://bugcrowd-tc.instructure.com/courses/XXX/pages/YYY`	915faf88da81fd695c5d34b9e52354f13b350a1a82a16620260bb21914f7ca69	2	$868.96	Resolved
View information of all users - `https://bugcrowd-tc.instructure.com/api/v1/sections/XXX/enrollments`	5b92944c21ab3ee2b410725f85a570c76a4d9ee4beb5748b76fab61a649a118d	2	$868.96	Resolved
CSRF to create a new quiz - `https://bugcrowd-tc.instructure.com/courses/XXX/quizzes/new`	403003b02ea091d17dcbf7eecd03c0a8e596d04391ddd3a50ec4a802cf17675c	3	$434.48	**Unresolved**
IDOR - Any User Can Send Invitation to All Users	b2ed86d6702d119f259ad1179057e246e2b6e6640da8bca2ab65d84494c01d1e	3	$434.48	**Unresolved**
IDOR to associate a quiz with any rubric - `https://bugcrowd-tc.instructure.com/courses/XXX/rubric_associations`	3c4518e3705041f25358f99f8860d2fecdae855c4643c9c3779951e96c888583	3	$434.48	**Unresolved**
Reflected XSS via tool_consumer_url on /courses/113/lti/tool_proxy_registration	d8d80d46b827e96ced6ff4c23a03e59cf3611a2a6706fac4fd989375b623e047	3	$434.48	**Unresolved**
Stored URL redirection	71874a7668f5ebd84401b5f995e8437c044b7d9db329a8d8176846d652af4799	3	$434.48	Resolved

Unauthenticated access to any Arc file when knowing the filename - `https://bugcrowd-tc.test.instructuremedia.com/api/file_service/file_upload_policies/s3_url_signature.json`	177f3cd9c730c17d7c2153b25cc223377f3c6909b693cf9a18fbe525edcc4c6f	3	$434.48	Resolved
View events of unpublished courses	cde218e9f0f420812506543e5e9736d97fd900e1e7ac19b38e1a9de144eeb78b	3	$434.48	Resolved
View information of all users - `https://bugcrowd-tc.test.instructuremedia.com/api/media_management/perspectives/XXX/perspective_permissions/batch_update`	4b903030025da73cd03a3fd1a5df5fd63d47d227b44d59119cb2ece08da7ce30	3	$434.48	**Unresolved**
XSS in `https://bugcrowd-tc.instructure.com` via Flash	2332253d9795b806ef2ea05b90f162f64617dbc4b8adfe62c5c1edf059b6ca93	3	$434.48	Resolved
Detailed Error Gives Full Operating System Path	b950769fbb9258ad246699cb3ed63726f576856fa115363ed8297aa1708334f7	4	$200.00	**Unresolved**
External SSRF via Link Validation	e97336973a308bbd5ef92e4c230bb5239f17c87a42a24cc292f118ce06450087	4	$200.00	Resolved
Information Disclosure SQL Query	636876e5d66ae5d054e8a27bfa18ddcc6fc56d453f62a262bfb224a4e816c173	4	$200.00	**Unresolved**
Local path disclosure - `https://bugcrowd-tc.test.instructuremedia.com/api/file_service/file_upload_policies/s3_url_signature.html`	e766c6800ae15e3a11110a768cef0d688e7b6d5c06eee81f182dc03b8090e4a3	4	$200.00	**Unresolved**
Open Redirect	1b2559414d6cdfa684b8309dd0592730793210d2a510a3df4ae334ce89aed2a7	4	$200.00	**Unresolved**
Open redirect at `https://bugcrowd-tc.instructure.com/courses/368/external_tools/retrieve` (url)	faac63e74e5ee0ad1e9720996ba8520060fd5cda95e6f666bacc70ea418e9298	4	$200.00	**Unresolved**
Post Comment in Private Portfolio	1e284ee5810177de67df47df1f5f274fa9d523cbac06dc75461eea92b9f4eb1f	4	$200.00	**Unresolved**
SSRF at `https://bugcrowd-tc.instructure.com/api/v1/courses/1970/external_tools`	af9010c6c4d6bc7a4c3c18bb319f07ff5321fe43eb80559be1fb66a8b0029a29	4	$200.00	Resolved
SSRF at `https://bugcrowd-tc.instructure.com/courses/1956/assignments/457/submissions`	255750c458d9d35933ac6437b115f309b6f6c38eece15bf54cedf250fd0efee2	4	$200.00	**Unresolved**

SSRF at `https://bugcrowd-tc.test.instructuremedia.com/api/media_management/media/71`	bdbd1701bb28ba7f4dd5b3f268df8687acb3322c420a6fdd7476292d54ad5cef	4	$200.00	**Unresolved**
SSRF via endpoint parameter on external_content_controller	b5601a318924813557d3420b6e3f807037557b5816f02e93baeb5359900a15d4	4	$200.00	**Unresolved**
Spoof Content at `flashmediaelement.swf`	d5bceb3ee751fe13de041fe398cb65ca9852724971ca388018f7b5f1c2c10176	4	$200.00	Resolved

Document History

- April 6, 2017 – Document Created