bugcrowd

Instructure's Canvas

Bugcrowd Flex Program and Retest Results

March 24, 2016

Executive Summary

Instructure engaged Bugcrowd Inc to perform a Flex Bounty Program (”Flex”), commonly known as a crowd-sourced penetration test, on **Instructure’s Canvas**. Testing occurred during the period: **11/17/2015** – **12/11/2015**.

For this Flex, **56** researchers were invited to participate; **45** accepted the invitation, resulting in **138** vulnerability submissions received from **26** unique researchers. These issues ranged in scope and severity, with **3** high priority **P2** issue(s) discovered. As a whole, researchers with rewardable submissions received **$19,300** out of a total prize pool of **$20,000**.

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 on Bugcrowd Flex programs.

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

Reconnaissance
Enumeration
Documentation
Exploitation

- **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**.

Priority Key

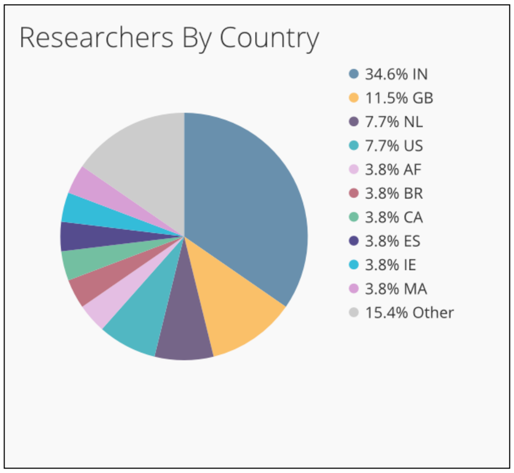
The following priority matrix is used as a guideline to classify valid assessment findings:

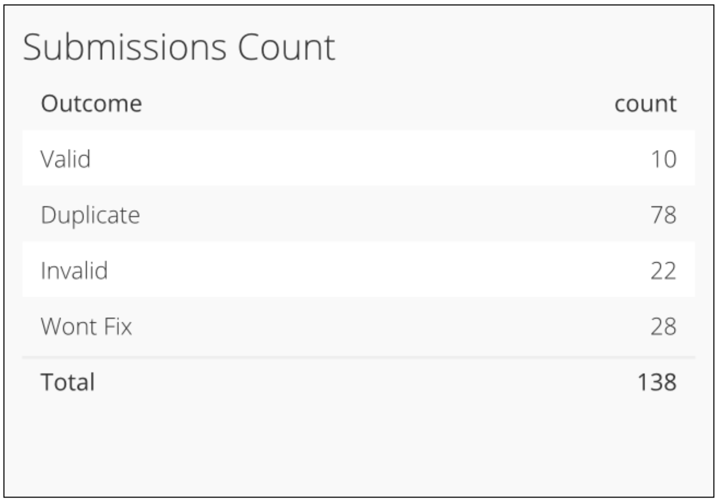
Priority	Impact	Example Vulnerability Types
P1 – Critical	Vulnerabilities that cause a privilege escalation from unprivileged to admin or allow for remote execution, financial theft, etc.	● Remote Code Execution ● Vertical Authentication Bypass ● XML External Entities Injection ● SQL Injection ● Insecure 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

Flex Bounty Program Overview

A Flex 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 Flexes 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 Flex for **Instructure's Canvas** received submissions from **26** researchers in the following countries: **Afghanistan, Brazil, Canada, India, Ireland, Morocco, Netherlands, Philippines, Portugal, Romania, Spain, Turkey, United Kingdom, and the United States**. Most of the researchers are based in **India**.

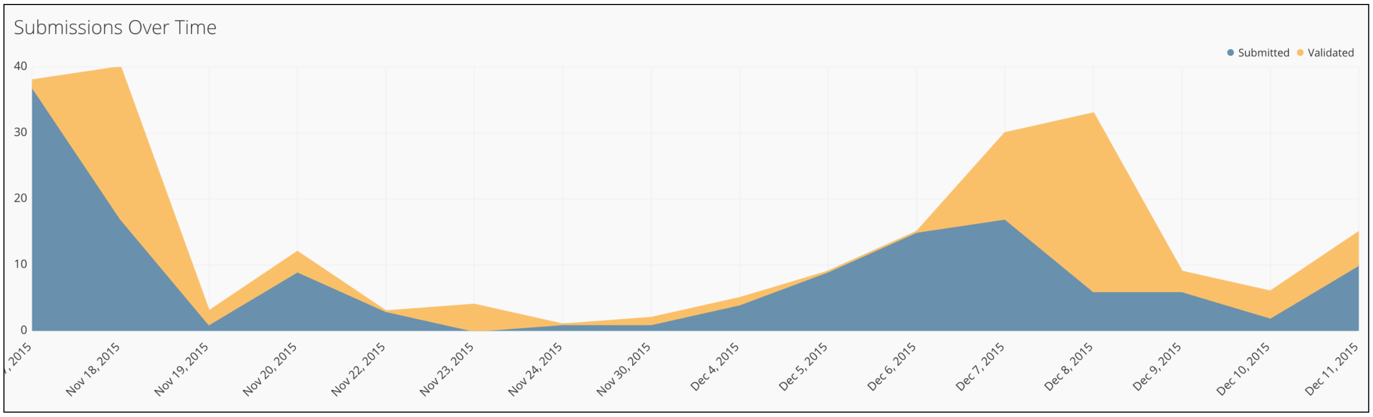

Researchers By Country


Submissions Count

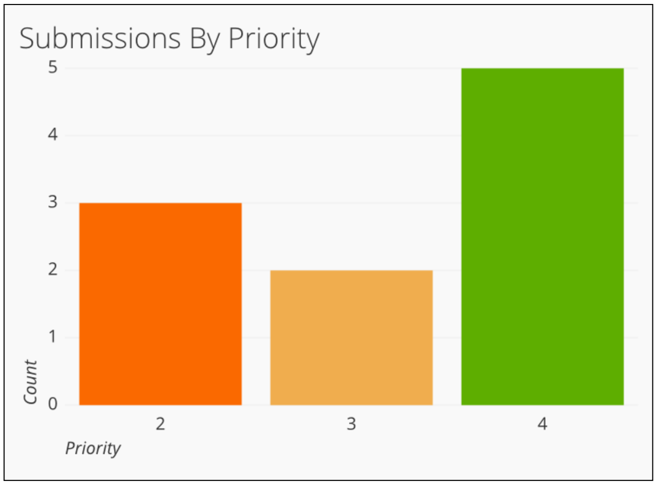
Outcome	count
Valid	10
Duplicate	78
Invalid	22
Wont Fix	28
Total	138

A total of **138** submissions were received, with **10** unique valid issues discovered. Bugcrowd identified **78** duplicate and **28** won't fix submission(s), and removed **22** invalid submission(s).

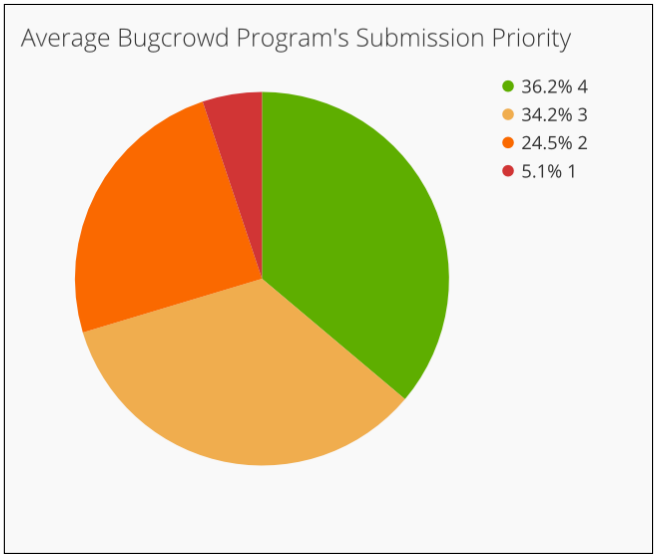
The timeline below shows submissions received and validated by the Bugcrowd team:

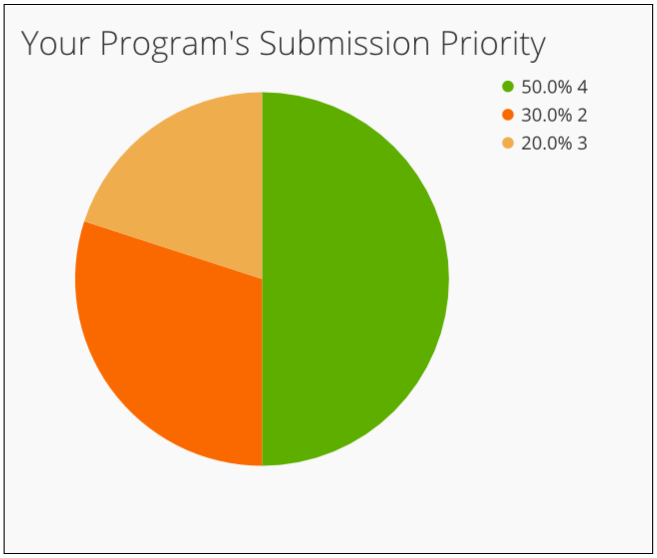

Submissions Over Time

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's Canvas** Flex were **P4**.



A comparison of Bugcrowd's other flexes to the the **Instructure's Canvas** Flex is shown below.





All Valid Submissions

Title	Reference Number	Priority	Reward	Retest
Stored XSS via Groups	de61564ce42f9e9013c100f14031da9392d5f60b081a886f0c0ce605af56d7a0	2	$6,000.00	Resolved
Stored XSS via Outcomes	7391ca90e0fdf157143b12e0c602aa14a03d21e6ec129f80171ab9dcc1ed3284	2	$4,000.00	Resolved
Stored XSS in Quiz Question Bank as Teacher	1fd8f1db7cbd2a8d6076802b40cb8993438cea6cdd93b7c2b6440d8ab1ca7c19	2	$3,000.00	Resolved
Privilege escalation via IDOR : Change the behalf of another user All Notification Preferences	e31b26d4fe28dc894b4d7a116523f6b69387cc397cd63fff4466ed38cbfd0b75	4	$500.00	Resolved
Content Spoofing (iframe Injection via HTML Editor)	f224e7c58b711457bb73610d7853a5c5f27e25cfc7e43de2b220155a5dcb391e	3	$200.00	Resolved
User account information IDOR at /users/<user_id>	7d2e91c088b03ebc71ee33504832ebe572ecd8f84bc827e9e67cdffaf304e7ac	3	$200.00	Resolved
CSV Injection (Gradebook Export)	8944ad7281953f597cf6091becbeba36fbfda5dcddb745947c4ccfd14e172e1b	4	$200.00	Resolved
Course Page IDOR	90332ea307577359de9d50b47e0b97a112f50c26b6646416c4920017bbed518b	4	$200.00	Resolved
External Authentication Injection via HTML Editor	d8989daebdedcacaf512bf1312bfe1d9cfd44979359a833a58dda704a1012885	4	$200.00	**Unresolved**
Window Opener Property Bug via HTML Editor	3d253e7e68775ab8e17b8dfbca01d417fe5d59f1ca264f2ce933fb5c5541c8e3	4	$200.00	Resolved

Document History

- March 24, 2016 – Document Created