bugcrowd

CANVAS by Instructure

Bugcrowd Flex Program Results

December 2014

Executive Summary

Bugcrowd Inc was engaged by Instructure to perform a Flex Bounty program, commonly known as a crowdsourced penetration test, on the CANVAS infrastructure and source code. The testing was performed between October 08 – 22, 2014.

During the test, 322 submissions were received from 63 unique testers. From these submissions, 59 unique security issues were identified over the course of the two week testing window on the Instructure CANVAS staging environment. These issues ranged in scope and severity, with no critical issues discovered. The primary finding was a prevalence of Stored XSS vulnerabilities, which have now been remediated by the Instructure team.

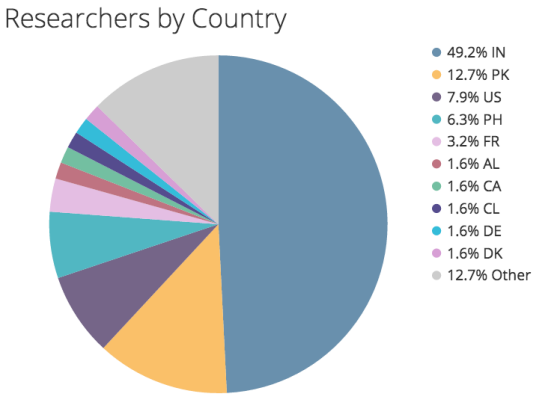
While there were a large number of issues found in comparison with previous tests run against the CANVAS infrastructure, this is expected with a Bugcrowd Flex Bounty. On average, 73 findings are found and reproduced in programs against applications of similar size and scope. The Flex Bounty program for CANVAS produced 59 findings, a significantly lower number compared to other programs.

Given data collected while performing Flex Bounty programs for organizations of similar size and scope, it is Bugcrowd's assessment that the CANVAS application was designed and developed by engineers who possess an understanding of best practices. The security team's vulnerability response during and after the program was organized and well thought out. Based on our experience working on bounty programs, the Instructure team takes security seriously.

Flex Bounty Program Overview

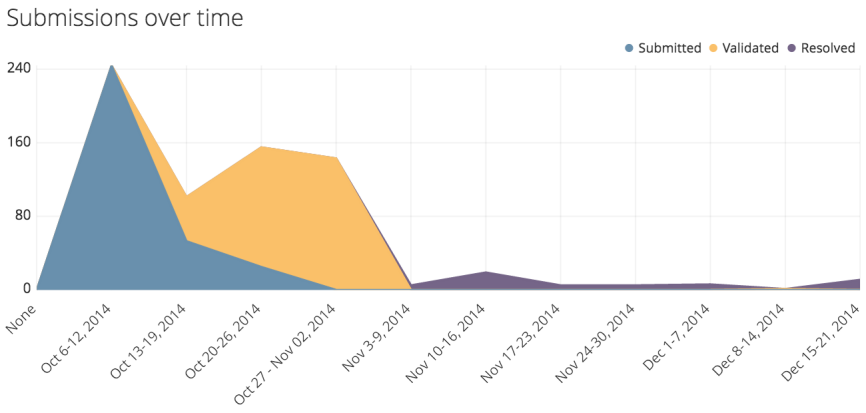
A Flex Bounty program is a novel approach to an application assessment or penetration test. Traditional penetration tests use only one or two researchers, resulting in less overall testing of the application. Bugcrowd researchers routinely examine applications and discover many esoteric issues that automated testing cannot find and that traditional vulnerability assessments routinely miss.

The Flex Bounty program for CANVAS had 63 invited researchers testing the application, from an array of countries around the world.



Outcome	Count of Submissions
DUPLICATE	125
IGNORED	41
INVALID	97
VALID	59
Total	322

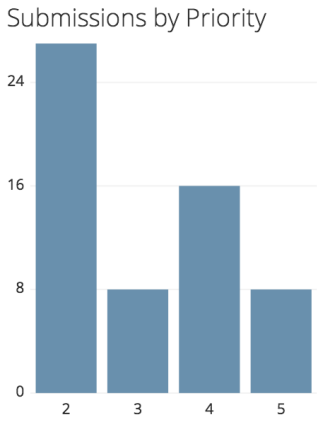
59 valid and reproducible issues were identified out of 322 total submitted issues. Bugcrowd cleaned all data, removing ignored, invalid, and duplicate issues.

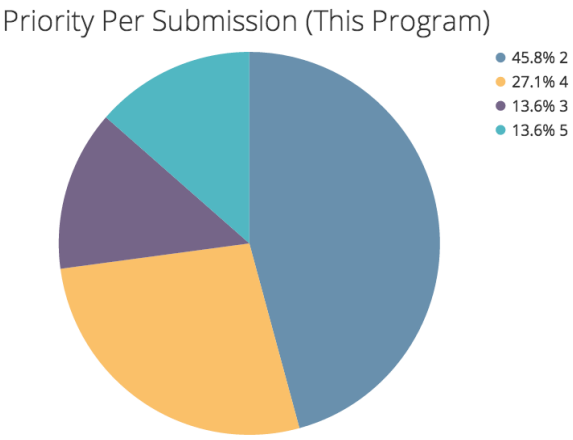


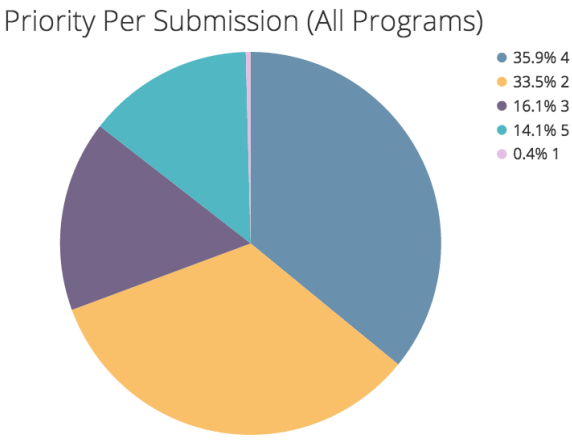
To the left, the timeline demonstrates submissions received, validated, and then finally resolved during the program by the Instructure team. In combination with the lack of critical findings, it is this final step, resolution, that indicates a mature security program for CANVAS.

Bugcrowd ranks the technical priority of all confirmed findings on a scale from 1 (critical) to 5 (accepted risk). The results can be found to the right. There were no critical issues identified.

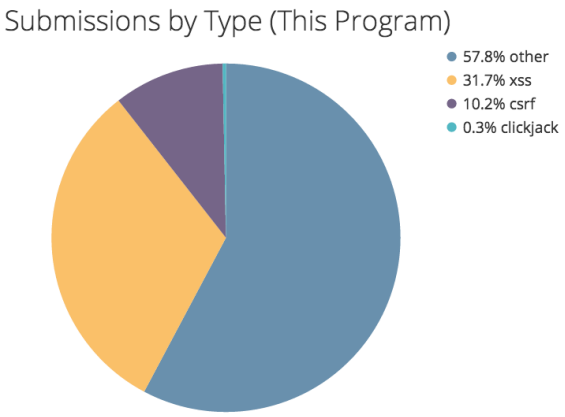
The comparison of this program to other Flex Bounty programs on Bugcrowd's platform is below. The stored XSS findings make the Priority 2 ratio slightly higher than other programs but there were no priority 1 issues found and fewer overall findings (59 vs. 73 in other comparable programs)

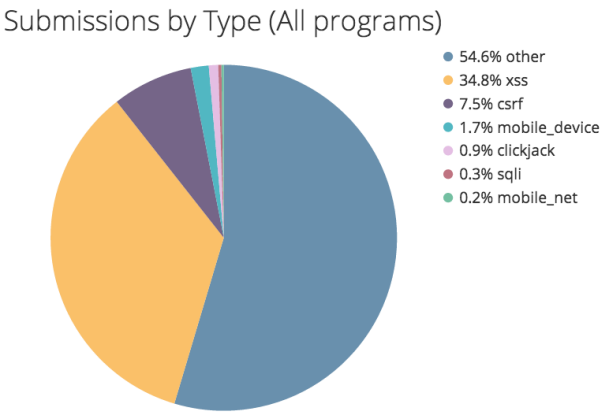






Above, the overall finding types are compared with other programs of similar size and scope.





Valid submissions on this program averaged a $162.75 payout, with the maximum payout being $2000. A total of $8300 was paid out during the course of the two-week program.

Priority Key

The following priority matrix was used to classify the Instructure CANVAS assessment findings.

Priority Level	Common Name	Description	Examples
P1	Critical	Vulnerabilities that affect all users of the platform, and / or affect the security of the platform or host system(s).	Remote code execution Vertical authentication bypass SSRF XXE SQL injection
P2	High	Vulnerabilities that affect more than one user of the platform, and that require little or no user interaction to trigger.	Stored XSS Direct object reference User authentication bypass
P3	Medium	Vulnerabilities that affect more than one user, but may also require interaction or a specific configuration.	Open Redirect, Reflected XSS, CSRF
P4	Low	Issues that affect singular users and require interaction or significant prereqs (MitM) to trigger.	Common flaws, Debug information, Host Header

Findings Summary Matrix

Finding Name	Priority	Finding Status	Instructure Response
3 stored xss in discussions	2	Resolved	Fixed.
3 stored xss in same place (teacher account in syllabus area)	2	Resolved	Previously fixed in production.
Content Spoofing on uploadify.swf	2	Resolved	Upgraded to latest version, fixed.
CSRF in email addition	2	Resolved	Ultimately a false positive.
Flash Based Cross Site Scripting (Flash exploit)	2	Resolved	Fixed. Only reproducible in the test environment.
Flash XSS at rapid7-tc.instructure.com/ Filename: FileAPI.flash.image.swf	2	Resolved	Fixed.
Open Direct and XSS at https://rapid7-tc.instructure.com/images/users/1?fallback=http://www.bugcrowd.com/	2	Resolved	Ultimately, no sensitive data can be exposed by this XSS.
Quiz IP Filter bypass	2	Resolved	Fixed. Only reproducible in the test environment.
Reflected xss	2	Resolved	Fixed.
stored cross-site-scripting in https://rapid7-tc.instructure.com/eportfolios/19/Home/Welcome	2	Resolved	Fixed. Only reproducible in the test environment.
stored in files upload	2	Resolved	Fixed. Only reproducible in the test environment.
stored xss	2	Resolved	Fixed.
stored xss	2	Resolved	Fixed.
Stored xss	2	Resolved	Fixed.
Stored XSS	2	Resolved	Fixed.
Stored XSS	2	Resolved	Fixed.
Stored XSS - Calendar undated items	2	Resolved	Fixed (same underlying issue).
stored xss in calendar title	2	Resolved	Fixed.
Stored XSS in filename in Tooltip of Calendar Events	2	Resolved	Fixed.
stored xss in https://rapid7-tc.instructure.com/dashboard/files	2	Resolved	Fixed. Only reproducible in the test environment.

Finding Name	Priority	Finding Status	Instructure Response
Stored XSS - Possible answer Quizzes	2	Resolved	Fixed. Only reproducible in the test environment.
xss	2	Resolved	Fixed.
XSS	2	Resolved	Not a viable attack vector (Self-XSS). Plan to fix anyway.
Xss in Enrollment	2	Resolved	Fixed.
xss in https://rapid7-tc.instructure.com/	2	Resolved	Fixed.
Xss in Import Content	2	Resolved	Fixed.
XSS via File Upload SWF	2	Resolved	Fixed. Only reproducible in the test environment.
Assigning more than prescribed students in a group	3	Resolved	Not a security bug. Fixed. Group limits are respected when students are randomly assigned.
Failure to Restrict URL Access	3	Resolved	Ultimately not a viable attack vector. Complexity of brute force protection is sufficient.
Forced Browsing by teachers to access unauthorized groups	3	Resolved	Working as intended.
No rate limiting on conversation messages	3	Resolved	Rate limiting being added.
Sending messages for unsubscribed courses	3	Resolved	Fixed.
Sending messages from unsubscribed groups	3	Resolved	Fixed.
Unauthorized access to announcements	3	Resolved	Ultimately not a viable attack vector. Complexity of brute force protection is sufficient.
Xss in Quiz	3	Resolved	Fixed. Only reproducible in the test environment.
Accepting Old Password As New Password	4	Resolved	Fixed. Only reproducible in the test environment. Best practice for OSS version updated.
Encrypted Cookie Store malleability / Key-reuse	4	Resolved	Updated cookie store gem. Fixed in next release.
Force-Login CSRF on CANVAS	4	Resolved	Fixed.

Finding Name	Priority	Finding Status	Instructure Response
Host header attack	4	Resolved	Fixed. Only reproducible in the test environment.
X-Forwarded-Host Host header Attack	4	Resolved	Fixed. Only reproducible in the test environment.
Missing DNSSEC	4	Resolved	Not a viable attack vector.
No rate limitation on email confirmation	4	Resolved	Not a viable attack vector.
No validation on add email function (POST /communication_channels)	4	Resolved	Fixed.
Password Complexity very low.	4	Resolved	Working as intended. Not an issue in production.
Privilege escalation in calender	4	Resolved	Ultimately not a viable attack vector. Complexity of brute force protection is sufficient.
Sending Message from other user id	4	Resolved	Not a viable attack vector.
Session Timeout Not Implemented in the application	4	Resolved	Working as intended (24 hour timeout by default).
SPF issue	4	Resolved	Working as intended. Not an issue in production.
ssl 3.0 poodle attack	4	Resolved	Fixed. Only reproducible in the test environment.
Stored XSS	4	Resolved	Fixed (same underlying issue).
Unsafe delete on params hash	4	Resolved	Not currently a viable attack vector. 8 Patches deployed. Coding practices updated.

Document History

- January 12, 2015 - Document updated with finding clarification, remove image placeholders.
- December 20, 2014 - Clarification on number of findings vs other programs.
- December 19, 2014 - Document updated for public release.
- October 31, 2014 - Document updated with participation information.
- October 31, 2014 - Document created.