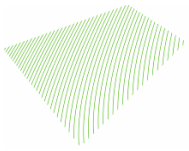
CANVAS APPLICATION PENETRATION TEST SUMMARY

INSTRUCTURE

December 2012

Version 1.1
Project Reference: SG-1591-12

SecurusGlobal



Copyright

Engagement Representatives

Drazen Drazic CEO, Securus Global		Phone: +61 2 9283 0255 Email: drazen.drazic@securusglobal.com

Revision History

12 November 2012	v0.1	Document Creation
13 November 2012	v0.2	Technical QA
14 November 2012	v1.0	Non-Technical QA and Initial Release
18 November 2012	v1.1	Updated After Re-Testing

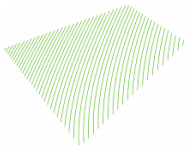
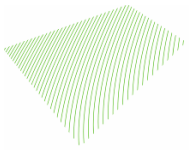


Table of Contents



1 EXECUTIVE REPORT

1.1 Executive Summary

This report presents the findings of a security assessment of Instructure's Canvas platform conducted from 31st October 2012 to 5th December 2012.

This environment was comprised of a single open source web application which was available in both shared and dedicated environments. The purpose of this testing was to provide Instructure with an understanding of the security posture of the Canvas platform with a focus on recent modifications to the source code.

Overall, the security posture of the environment is reasonable, with several high and medium vulnerabilities being identified in the application during testing. However, as a result of reporting of issues promptly and regular status updates, all high risk issues were resolved with a number of moderate and low risk vulnerabilities also being resolved.

The Canvas platform has largely been developed with security in mind, as most forms and user supplied input are heavily validated and restricted. The platform was developed on top of the Ruby on Rails MVC framework which provides a strong security baseline. There are, however, some improvements that could be made to the code base that could reduce the likelihood of introducing new vulnerabilities in the future.

Additionally, issues that have had their risk accepted in the past were identified to still exist within the platform. It is recommended that the acceptance of these risks be regularly reviewed as part of a regular risk assessment process.

The remaining issues present a moderate risk to the integrity and confidentiality of the stored data which could lead to reputational damages and loss of confidence in the CANVAS system should they risk be realised. None of these issues are associated with major application flaws that are difficult to remediate.

1.2 Document Scope

This report consists of the following components:

- Summary Report: A report targeted at senior executives and business stakeholders that presents a summary of the project, findings, and recommendations.
- Appendices – Supplementary information supporting the report including our risk assessment methodology and matrix.

1.3 Disclaimer

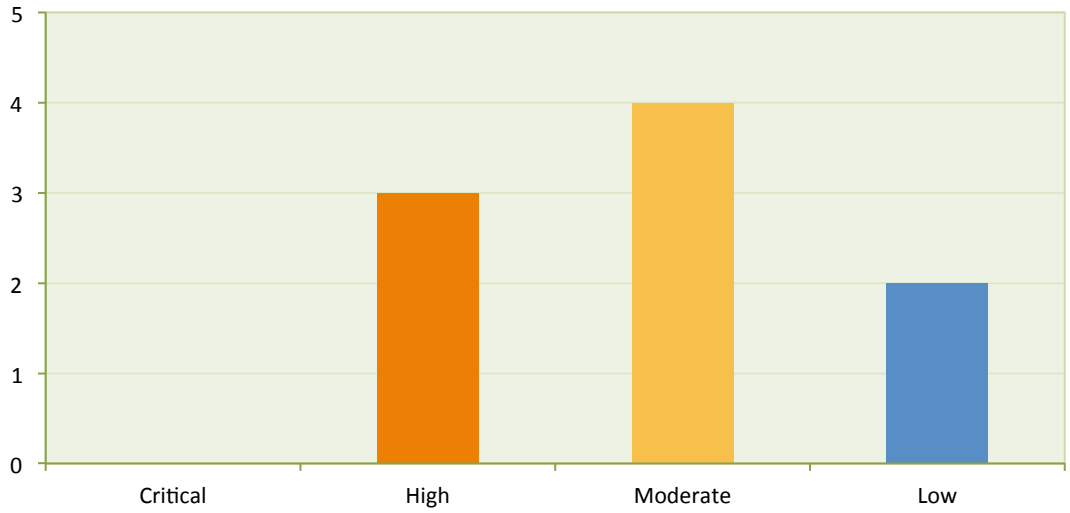
This security test is a point in time assessment of the state of security in the Canvas platform, valid at the time that the test was completed. The description of the findings, recommendations and risk will be valid for the time of the test. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence.

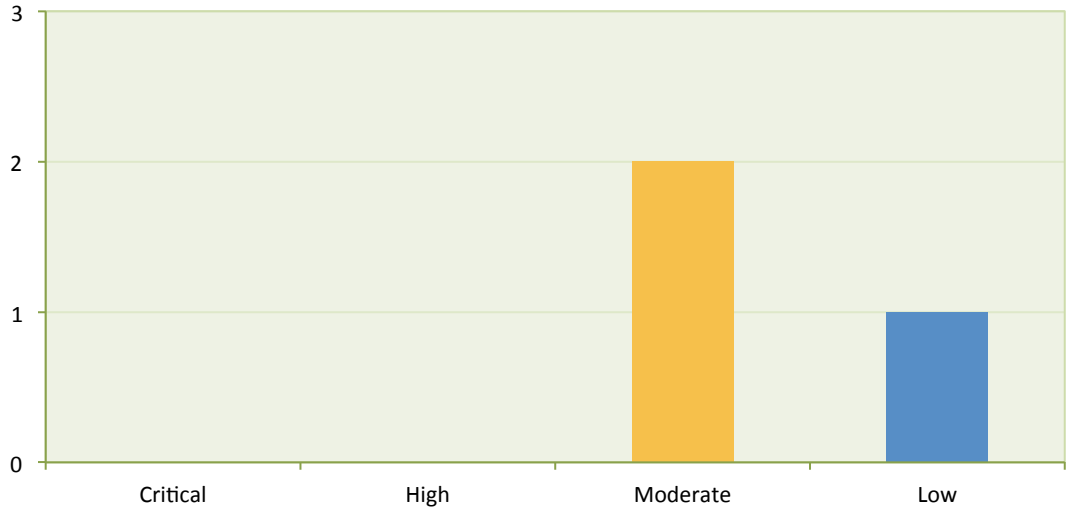
1.4 Summary of Findings

Following in depth testing of the environment it is our impression that the CANVAS application is robust and has been developed by security aware programmers in line with secure coding practices.

Based on our understanding of your business, we have assessed the level of risk to your organisation based on the nature of the vulnerabilities discovered, their exploitability in your environment and the potential impact should the risk be realised.

The following graphs illustrate the levels of risk for the vulnerabilities identified during testing and the residual risk following the vulnerabilities being addressed:

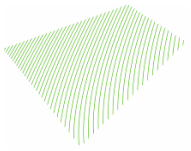




1.5 Summary of Recommendations

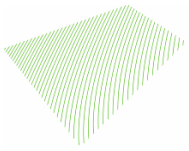
To address the identified issues it is our recommendation that:

- XML parsers should be configured to prevent the use of external entities
- Apply strict whitelisting and retrieve the base name of user input before being included in a file path
- Upper and lower limits are placed on all numeric inputs into the application



- An upper limit is placed on the number of files a ZIP file can contain
- Script resources residing on HTTP are not referenced inside content served over HTTPS
- Protection against brute-force and replay attacks are implemented on the two-factor authentication component
- Replace string concatenation with parameterised queries when constructing SQL queries
- Sequential values used within URLs are cryptographically signed by the application
- Review the risk acceptance of issues that still exist from the first security review.

For a detailed description of our findings and recommended actions, please refer to the section entitled: 'Technical Report'.



1.6 Summary of Vulnerabilities

The following tables are a summary listing of the vulnerabilities discovered through our testing, including the status as of December 18th 2012, and the time to fix the vulnerabilities in the live CANVAS application.

1.7 Tables of Findings

Canvas Application

	Finding	Risk	Status	Time to Fix
2.2.1.	XML External Entities (XEE) are not disabled	**High**	Fixed	~ 1 day
2.2.2.	User Controlled File Path	**High**	Fixed	~ 1 day
2.2.3.	Denial of service through file upload	**High**	Fixed	~ 2 weeks
2.2.4.	Insufficient Data Validation	**Moderate**	Fixed	~ 2 weeks
2.2.5.	Application mixes both HTTP and HTTPS content	**Moderate**	Fixed	~ 2 weeks
2.2.6.	Two-factor authentication is not implemented correctly	**Low**	Scheduled	-
2.2.7.	Insecure Coding Practices	**Informational**	N/A	-
2.2.8.	Information disclosure via parameter tampering	**Informational**	N/A	-
2.2.9.	Arbitrary File Read	**Informational**	Scheduled	-

Outstanding Issues from 2011

	Finding	Risk	Status	Time to Fix
2.3.1.	Arbitrary File Upload	**Moderate**	N/A	-
2.3.2.	Autocomplete Enabled for Sensitive Data	**Moderate**	N/A	-
2.3.3.	Cross-Site Request Forgery	**Low**	N/A	-

2 APPENDICES

2.1 Risk Classification

Securus Global follows the International Standards ISO 31000 and ISO 31010 for risk identification, classification and assessment. The following classification matrixes have been used to derive likelihood and impact.

2.1.1 Risk Matrix

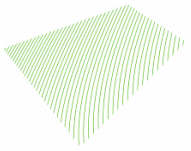
Likelihood	Consequence				
	Insignificant	**Minor**	**Moderate**	**Major**	**Significant**
Almost Certain	Low	Moderate	High	Critical	Critical
Likely	Low	Moderate	Moderate	High	Critical
Possible	Low	Low	Moderate	High	Critical
Unlikely	Low	Low	Moderate	Moderate	High
Rare	Low	Low	Low	Moderate	High

2.1.2 Risk Classification

Rating	Description
Critical	Immediate action required
High	Senior management attention needed.
Moderate	Management responsibility should be specified
Low	Manage by routine procedures

2.1.3 Likelihood Description

Likelihood	Description
Almost certain	It is almost certain expected to occur in most circumstances
Likely	Will probably occur in most circumstances
Possible	Might occur at some time
Unlikely	Could occur at some time
Rare	May occur only in exceptional circumstances



2.1.4 Consequence Descriptions

Consequence	Description
Significant	May cause extended system outage or may result in complete compromise of information or services.
Major	May cause considerable system outage, and/or loss of connected customers or business confidence. May result in compromise of large amount of information or services.
Moderate	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. It will require expenditure of significant resources to repair.
Minor	Will result in some tangible harm, albeit negligible and perhaps only noted by a few individuals. Will require some expenditure of resources to repair.
Insignificant	Will have little or no impact if threat is realised and the vulnerability is exploited.