# CANVAS SECURITY ASSESSMENT SUMMARY

INSTRUCTURE

December 2011

Version 1.1
Project Reference: SG-1472-11

SecurusGlobal

## Copyright

## Engagement Representatives

| | |
|---|---|
| Drazen Drazic<br>CEO,<br>Securus Global | Phone:+61 (0) 2 9283 0255<br>email: drazen.drazic@securusglobal.com |

## Revision History

| | |
|---|---|
| V0.1 | Findings and business analysis included |
| V0.9 | Quality Assurance Review |
| V1.0 | Draft for Discussion Report released |
| V1.1 | Amendments following walkthrough |

## Table of Contents

# 1 EXECUTIVE REPORT

## 1.1 Executive Summary

This report summary presents the findings of a security assessment of Instructure's Canvas platform conducted between the period 7th November 2011 to 25h November 2011.

It is our impression that CANVAS is generally a secure application and that the issues found can quickly be remediated. CANVAS is built upon a foundation of very widely used programming frameworks that have been subject to extensive security auditing.

During testing several issues were identified, including one critical vulnerability. Due to progressive reporting and status updates with Instructure the critical vulnerability identified was promptly remediated and released to users.

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 test environment prepared for Securus Global 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 the Instructure business, we have assessed the level of risk to your organisation based on the nature of the vulnerabilities discovered, their exploitability in the environment and the potential impact should the risk be realised to be low.

There were no major design flaws identified. Vulnerabilities identified were of a nature that allowed remediation without major resign or application re-coding. During the testing a critical SQL injection vulnerability was identified. We also uncovered an issue with the way the application framework generated session IDs. Both vulnerabilities were fixed quickly in response to our reporting.

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

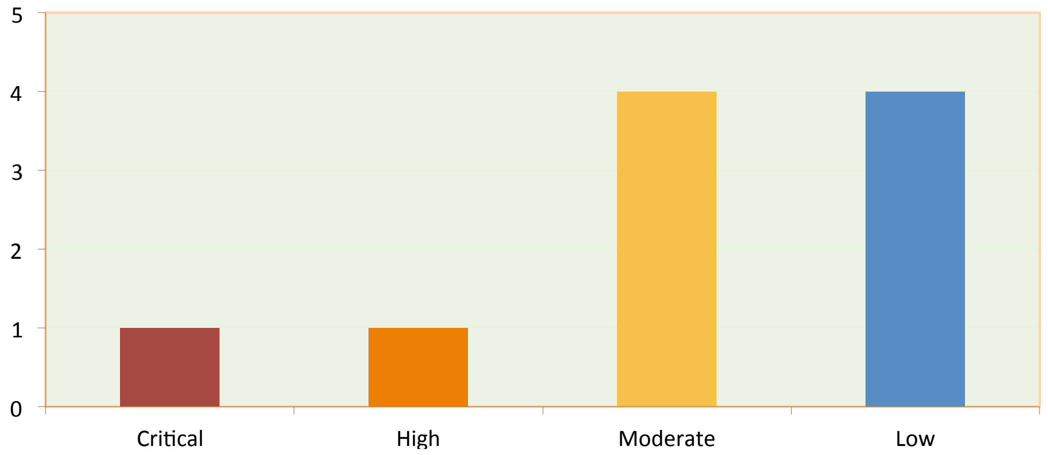

**Figure 1 Vulnerabilities identified during testing**

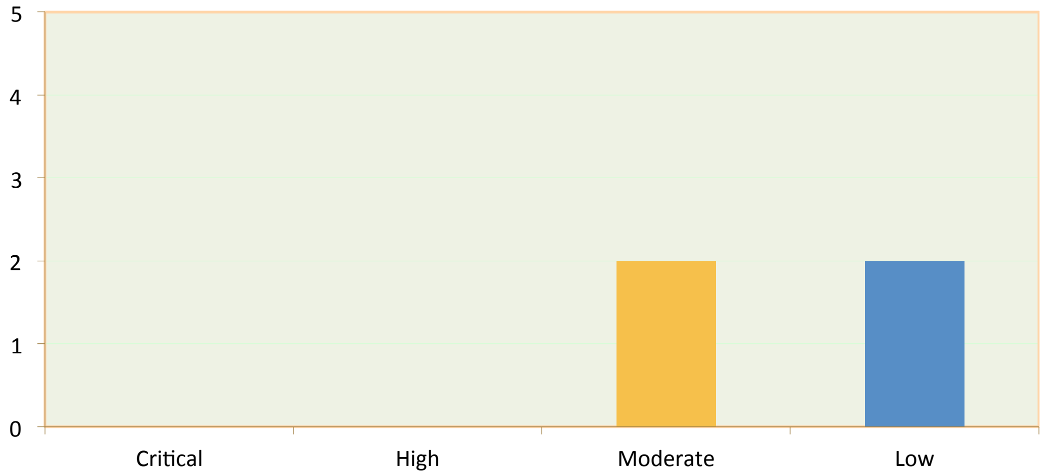

**Figure 2 Residual Risk following remediation of vulnerabilities during testing.**

## 1.5 Summary of Recommendations

To address the identified issues it is our recommendation that:

- The JSON interfaces are protected from cross-site reading
- File uploads are limited or handled safely
- Autocompletion of sensitive forms is turned off
- CSRF tokens are deployed wherever state-changing functionality is triggered
- Input to SQL queries is escaped and strict whitelisting is performed
- Allowed markup is restricted further
- Unauthenticated file access is disabled
- Uploaded files are scanned for malware before users are allowed to download them
- IDs are used to identify users when messaging a new user
- Service banners containing version/software information are censored
- A new session ID is created every time a user logs in

## 1.6 Summary of Vulnerabilities

The following table is a summary listing of the vulnerabilities discovered through our testing, including the status as of December 1st 2011, and the time to fix the vulnerabilities in the live CANVAS application.

## 1.7 Table of Findings

| | Finding | Risk | Status | Time to Fix |
|---|---|---|---|---|
| 1. | SQL Injection Vulnerability Identified | **Critical** | FIXED | ~2 hours |
| 2. | JSON Interfaces Allow Cross-Site Reading | **High** | FIXED | ~2 weeks |
| 3. | Arbitrary File Upload | **Moderate** | FIXED | ~2 weeks |
| 4. | Autocomplete Enabled for Sensitive Data | **Moderate** | N/A | - |
| 5. | Cross-Site Request Forgery | **Low** | FIXED | ~1 week |
| 6. | Overly Permissive HTML Sanitisation | **Moderate** | Scheduled | - |
| 7. | No Access Control for Uploaded Files | **Moderate** | Scheduled | - |
| 8. | No Anti-Virus Solution in Use | **Low** | Scheduled | - |
| 9. | Conversation Delivery Name Spoofing | **Low** | FIXED | ~4 weeks |
| 10. | Incorrect Session Management | **Low** | FIXED | ~2 weeks |
| 11. | Information Disclosure Identified | **Informational** | FIXED | ~1 week |
| 12. | Partial Regular Expression Matching | **Informational** | 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

| Consequence | 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 vulnerability is exploited. |