High Level Security Assessment of the Canvas and Moodle Learning Management Systems

---

Background

Learning Management Systems (LMS) are integral to institutes of higher education. They help facilitate the dissemination of course materials, facilitate communication between students and faculty, and can track and quantify student learning. The purpose of this document is to do a high level security assessment of the two LMS packages:

- Moodle - https://moodle.org/
- Canvas - https://www.canvaslms.com/

The assessment will be based on both the best practice security protections built into each product and previous third party research done with regard to vulnerability datasets. The previous research provides an analysis of the number of vulnerabilities discovered and the severity of the vulnerabilities based on the International Standards ISO 31000 and ISO 31010 for risk identification, classification, and assessment. The overall security baseline for web based applications is that they are going to have vulnerabilities.

Canvas

Canvas LMS' web frontend is based on Ruby on Rails with a backend database built upon PostgreSQL. Offered mainly as a hosted cloud based service, Canvas LMS can also be installed and hosted locally. The infrastructure must be properly installed and maintained, which includes appropriate patching, log review, and role based access controls. Utilizing the cloud service also provides for faster patching and low down time. Ruby on Rails web development creates added encapsulation that adds an ease of web platform vulnerability patching. Canvas also supports the use of LDAP integration. Using LDAP integration with Canvas enables the enforcement of password complexity and expiration based on site policies.

The codebase for Canvas LMS is open source, which allows for more in depth security reviews as well as an active community led improvement program. Instructure, the creator of Canvas LMS, has performed in depth third party security reviews every year since 2011, which has led to rapid implementation of vulnerability fixes and an overall positive security stance. As a result of these yearly security reviews and overall security posture, Internet2* has approved Canvas

LMS for General Availability as a Net+ application. Canvas is the first LMS to pass this security review and assessment using the Cloud Security Alliance Cloud Controls Matrix framework. Internet2 Net+ approval has also vetted provisions for Canvas LMS regarding FERPA and Business Associate Agreements under the HIPAA/HITECH data protection contractual obligations.
Internet2 is a not-for-profit United States computer networking consortium led by members from the research and education communities.

The 2014 vulnerability assessment yielded 59 unique validated bugs. 33 of those bugs were ranked 2 or lower, which could lead to information disclosure or privilege escalation. However, the 2015 assessment yielded 10 unique validated bugs, none of which being ranked critical. In both cases the vulnerabilities were fixed within 24 hours of the report release and reportedly had no impact on the users. Included in the testing were the mobile applications for iOS and Android operating systems. There are currently no known vulnerabilities for the mobile applications on iOS or Android.

Additionally, some of the key security features that Canvas supports:

- Full encryption for data at rest
- Multi factor authentication
- SOC 1/SSAE 16/ISAE 3402 certification
- HTTPS for all pages

Reporting a security issue:
“We take security very seriously. Please do not submit issues or pull requests for security issues. Instead, you can email security@instructure.com and we will respond as soon as possible. You can watch for security advisories to update your Canvas installation on our Security Notices forum.”

Moodle

Moodle has a php web frontend and is able to support MySQL, MariaDB, PostgreSQL, Microsoft SQL, and Oracle as the backend databases. The locally installed hosting infrastructure must also be properly installed and maintained, which includes appropriate patching, log review, and role based access controls. Using LDAP integration with Moodle will enable the enforcement of password complexity and expiration based on site policies. Additionally, using LDAP integration ensures that all of the content provided by Moodle will be sent via SSL instead of unencrypted communications.

Moodle makes use of community provided plugins for additional features and integrations. These plugins are published using the guidelines provided here:
https://docs.moodle.org/dev/Plugin_contribution_checklist

There are many different types of plugins and can be submitted by any developer. Many are not updated on regular intervals. The plugin based architecture opens security vulnerabilities that are not found in an LMS that keeps similar functionality tied to the core code.

The codebase for Moodle is open source, which allows for more in depth security reviews as well as an active community led improvement program. The Moodle base code is also highly customizable to meet the needs of the institution. This allows the site administrators to modify their local codebase to mitigate security vulnerabilities rapidly if they have the development resources. Moodle has declined performing third party vulnerability assessments and does not release results of internal testing and verification. In 2015 the MITRE Common Vulnerabilities and Exposures (CVE) database (http://cve.mitre.org) reported that there were 48 confirmed vulnerabilities reported. 43 of those vulnerabilities were ranked at level 4 or higher, which could lead to information disclosure or privilege escalation. There was limited data on how quickly these vulnerabilities were patched. If a critical vulnerability is discovered, the registered site administrators are notified in advance via email. Moodle released mobile applications in July, 2015. There are currently no known vulnerabilities for the mobile applications on iOS or Android.

Additionally, some of the key security features that Moodle supports:

- Full encryption for data at rest
- Multi factor authentication
- SOC 1/SSAE 16/ISAE 3402 certification
- HTTPS for all pages

Reporting a security issue:
“Create a new issue in the Moodle Tracker describing the problem (and solution if possible) in detail. Make sure you set the security level accurately to make sure that the security team sees it. Bugs classified as a "Serious security issue" or "Minor security issue" are hidden from everyone apart from the security team and the person who reported the problem. If you are not sure whether an issue is a security issue, you should still create a new issue in the tracker for review, using the security level "Could be a security issue".”

Additionally, Moodle is available as a cloud offering SaaS (Software as a Service) via Moodlerooms, the open source division of Blackboard. Moodleroom’s approved patching cycle aligns with the main Moodle application codebase. There are two major releases annually, as well as two maintenance releases in between each major release.
Moodleroom Moodle security vulnerabilities are addressed through emergency releases, and are “typically applied within one week from the corresponding stable release [from Moodle].” Moodlerooms correlates directly to the above assessment for Moodle, as the codebase is the same. The community provided plugin architecture is still utilized, with the ability to install insecure or no longer supported plugins. However, Moodlerooms has additional built in protections as the result of being housed in a ISO 27001 compliant public cloud services provider, Amazon Web Services, and performs internal and third party security audits on a undisclosed regular interval.

Summary

Yearly publically released security reviews, core functionality integration instead of community plugins, automated patching and the timeframe of patch releases makes the overall security stance of the default instance of Canvas higher than the default instance of Moodle.