Security Enhancements in Blackboard Learn 9.1 SP 10

Blackboard is committed to improving security features and resolving security vulnerabilities quickly and carefully. Such security vulnerability resolutions may lead to the release of a Security Advisory as well as any needed product update for our customers based on the context, severity and timing of confirmed vulnerabilities. Below we have outlined the security enhancements and security vulnerabilities resolved in this release.

Input Validation Filter

The Input Validation Filter is the new first line of defense to confirm data coming into Blackboard Learn is safe. It verifies that user requests coming in to the system are safe by sanitizing the data through a default ruleset. Administrators can create a custom ruleset to override a rule in the default ruleset and to decide which building blocks to apply the filter.

The Input Validation Filter is fast, providing cross-site scripting fixes much faster than the traditional patching process. Traditional patches can have various dependency issues or may need to be rolled back. Providing fixes through the Input Validation Filter is a much cleaner and faster way of delivering patches, as they are provided directly through the Software Updates Center.

The Input Validation Filter is installed and enabled by default for Blackboard Learn Release 9.1 Service Pack 10 and later. Access the Input Validation Filter feature on the Administrator Panel.

Alternate File Domain Settings for Serving Content

This security control forces files uploaded by users to open from another web domain. It is a defense-in-depth compensating control against potentially malicious files. It helps protect from Cross-site Scripting attacks performed through malicious files by leveraging the internet browser's existing security control, the "same-origin policy."

For example, your institution's main Blackboard site is `https://blackboard.myinstitution.com` and content is served from `https://blackboard-content.myinstitution.com` . By using an alternate domain, the user's cookies and session information is further protected from potentially malicious scripts in uploaded HTML files.

This security control is not enabled by default since it requires administrators to configure an alternate domain and its corresponding SSL certificate. Blackboard strongly recommends all customers enable this

setting.

Security API

Blackboard now is integrated with a best practices open source security library from the Open Web Application Project's (OWASP) Enterprise Security API (ESAPI). This security library is installed on Blackboard Learn through a building block called "ESAPI Security Module" and is required for system operation. Blackboard strongly recommends all building block developers leverage this new Security API based on OWASP ESAPI. These Security API changes include best practice implementations, and consistent nomenclature.

In later releases, the ESAPI Security Module Building Block API is part of Blackboard Learn's core code and is available by default.

Input influenced by users, whether trusted or not, needs to be validated on the server-side before processing (input validation). It also needs to be validated prior to display (output validation or escaping). Validation helps ensure system resiliency and prevents security issues such as cross-site scripting.

Input validation examples

```
ValidationUtility.isValidDirectoryPath( String )
ValidationUtility.isValidGuid( String )
ValidationUtility.isValidEnumeratedType( Enum, String )
```

Output Validation examples

Java Methods

```
EscapeUtility.escapeForHTML ( String )
EscapeUtility.escapeForHTMLAttribute ( String )
EscapeUtility.escapeForJavascript ( String )
EscapeUtility.escapeForUrl ( String )
EscapeUtility.escapeForCSS ( String )
EscapeUtility.escapeForXML ( String )
EscapeUtility.escapeForXMLAttribute ( String )
```

JSP Methods

```
${bbNG:EscapeForHTML( String )}
${bbNG:EscapeForHTMLAttribute( String )}
${bbNG:EscapeForJavascript( String )}
${bbNG:EscapeForURL( String )}
${bbNG:EscapeForCSS( String )}
${bbNG:EscapeForXML( String )}
${bbNG:EscapeForXMLAttribute( String )}
```

Cookie Security

Cookies for session management are hardened based on the persistence of cookie values, their associated IP addresses/relationships and lifecycle. Improvements include:

- Session cookies contain a secure flag set if SSL is enabled.
- Cookie values are reset on-expire, on-load, and on-login. For example, session management-related cookies are explicitly expired when the browser session is terminated or the session expires.
- Session cookie contains a httpOnly flag.

Cookie Disclosure Building Block

Blackboard is committed to ensuring that the collection, protection, use and storage of private information follows all legal and industry best practices by proactively supporting European Union regulations that help ensure privacy and security on the web. Blackboard is providing all Blackboard Learn clients with the Blackboard Security Management Cookie Disclosure building block. This building block allows schools to comply with the European Union's e-Privacy Directive. The building block can be downloaded and installed easily into Blackboard Learn instances.

The Blackboard Security Management Cookie Disclosure building block is intended to support the European Union Privacy Data Directive and laws implemented in the United Kingdom and other member states related to this directive. Specifically, this building block implements features that require users to provide consent prior to data collection and provides information about the nature and extent of data collection within Blackboard software and services to end users.

Security Fixes in this Release

There are over 100 client reported security fixes in this release. For details see the following KB articles available Behind the Blackboard:

- Cross-site Request Forgery
- Cross-site Scripting Fixes Requiring Global Safe HTML Filter Security Control (previously known as the Global Cross-site Scripting Security Control)

The "Global Safe HTML Filter Security Control" was previous called the "Global Cross-site Scripting Security Control". This is a pre-existing filter in the system and has been renamed to prepare for other security improvements. The security vulnerabilities described in the KB article are resolved in this release when the "Global Safe HTML Filter" is properly configured and set to the strictest setting. As a reminder, Blackboard recommends customers ensure the "Global Safe HTML Filter" Security Control is enabled and set to the appropriate settings. These controls are properly configured by default in SP10 and designed to neutralize user-controllable input before it is placed in output used by the application.

Other Security Fixes for Blackboard Learn SP10
