Security Enhancements in Blackboard Learn 9.1 SP 12

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.

For more information on each of the features and improvements, please see the System Administrator documentation.

Capturing Security Events - Central Security Log

High-level security events are now logged for auditing purposes. Events impacting security have been assigned security specific event codes. These event codes have been standardized within Learn. In SP12 these events codes have been introduced in predefined areas of application activity so validity may be demonstrated. For this release the authentication log will continue to be used to capture login attempts. For full security analysis, it is necessary to download all security-related logs, including, but not limited to, the Input Validation Filter log and the authentication log.

The types of security events captured cover high-risk activities enabling the tracking and source identification of the event through analysis of logged source internet address, source session, user id, and event time.

Log entries are based on industry standards for identification and description of security events that may be the result of system attacks making them suitable for importing/use-with third party tools for forensic analysis reporting. Additionally the logs themselves provide the ability for identification of specific events as immediately visible in the logs.

Log Location

```
Blackboard_Home/logs/security-validation-log.txt
```

Event Codes

These Event Codes are part of the Standard Security Event Codes.

Event Code	Security Event	Description
13	Invalid or Missing Cross-site Request Forgery Nonce Detected	Missing cross-site request forgery nonce for request authenticity and exception thrown. May be an indicator of a cross-site request forgery attack.
16	Invalid URL Redirection Detected	Invalid url in request and exception thrown. May an indicator of attempts to perform arbitrary redirects to malicious websites.
17	Invalid Resource Link in Course Package<resource in="" link="" passed=""/>	Invalid resource link in course package detected and ignored due to. May be an indicator of attempts to gain unauthorized access to resources.
23	Security Library OWASP ESAPI B2 Not Available but is called	Page not displayed and request not processed due to missing OWASP ESAPI Security Module B2 and exception thrown. Ensure the B2 is enabled since it is required. *In later releases, the ESAPI Security Module Building Block API is part of Blackboard Learn's core code and is available by default.*
24	Inline Receipt Message Signature Validation Failure Detected and Exception Thrown	Page not displayed due to missing inline receipt message signature and exception thrown. May be an indicator of attempts to perform phishing or cross-site scripting attacks.
26	Invalid Input Detected	Invalid input detected and dropped. May be an indicator of attempts to perform phishing or cross-site scripting attacks.

Secure User Password Storage

Blackboard Learn ships with an internal authenticator. This feature is oftentimes used by institutions that have not fully integrated with a third party authenticator such as LDAP or as a secondary authenticator for external users such as visiting faculty or parents.

Customers using a third party authenticator are excluded by this security control since user passwords are stored on an external system. However, the default system administrator account is in scope of this security control.

User passwords are stored by default with the salted SHA-512 standard from the SHA-2 family as defined in the National Institute for Standards and Technology (NIST) Special Publication 180-4 Secure Hash Standard. Blackboard Learn adds the best practice of "salting" using a secure random seed of HMAC-SHA-512. The practice of salting is important because it requires greater computing requirements to crack a password, in the event user password hashes are exposed to unauthorized actors.

Blackboard Learn also supports an alternative password hashing methodology that uses the Key Derivation Function (PBKDF2) Approach. PBKDF2 is part of a family of "adaptive hashes" that have gained popularity amongst the security industry for use with hashing passwords. This approach has a "slowness" factor about them that help provide resistance from password cracking. PBKDF2 is noted by the National Institute for Standards and Technology (NIST) Special Publication 800-132 Recommendation for Password-based Key Derivation.

Authentication attempts are logged into the standardized security log. Password storage scheme configurations and user password migrations to a new password storage scheme are also logged to the standardized security log.

Conditions for Internal Authenticator Secure User Password Storage

New Passwords

New passwords automatically use the new user password storage scheme by default as part of a secure design principle.

Pre-existing Passwords

Pre-existing passwords will automatically use the new user password storage scheme once the user logs in. Blackboard Learn cannot automatically migrate user passwords since passwords under the previous user password storage scheme were hashed. A new password hash can only be generated when the user logs in. Once the user logs in successfully and the password matches the previous user password hash value, the password is then automatically and seamlessly migrated to the new user password storage scheme. No user action is required. Once a password is successfully migrated, it will no longer be migrated again unless the default secure user password storage scheme changes to require it.

A security event is generated when a pre-existing user password successfully migrates. See the `Security Audit Logging` section.

How Passwords Are Stored

Passwords related to the internal authenticator are stored under the following format.

Format

```
{<Algorithm Family>}{}<Salt Algorithm>:<Hash Algorithm>:<Number of Hash Iterations>:<Salt Value>:<Password Hash Value>
```

Example password value using the default secure user password storage scheme

```
{SSHA}HmacSHA512:SHA-
512:3000:YHQ5mxGVxMwfsygj4WW1RVrAbciIVr7mGNcYiNq/zYTWASrUGEiGR87a2dRGL
Nc3PF4xnUxZPBe8TOg6T7lx8A==:zMb2jM6WoXJdfhG4O9uSBmht8tUM2oW+FOwiawqAqw
/tYZMuggdeEyeXROdVrc4gwJb9u+2PjtEwvs5ikQWDPg==
```

How to determine when pre-existing passwords have been migrated to the default Secure User Password Storage scheme

Pre-existing passwords under the legacy password storage scheme were stored in a legacy format. To re-iterate, new users or new installations of Blackboard Learn by default will use the secure user password storage scheme so no password hashes in the legacy format will appear.

Example password value using the legacy user password storage scheme

```
5EA9C3DB04B1C26A85FE7E541E7B3CD9
```

Example password value using the secure user password storage scheme

```
{SSHA}HmacSHA512:SHA-
512:3000:YHQ5mxGVxMwfsygj4WW1RVrAbciIVr7mGNcYiNq/zYTWASrUGEiGR87a2dRGL
Nc3PF4xnUxZPBe8TOg6T7lx8A==:zMb2jM6WoXJdfhG4O9uSBmht8tUM2oW+FOwiawqAqw
/tYZMuggdeEyeXROdVrc4gwJb9u+2PjtEwvs5ikQWDPg==
```

Secure User Password Storage Locations

Database

Internal authenticator user passwords are stored in the database `USERS` table.

No other passwords in the database are related to this Secure User Password Storage feature since this feature only covers credentials related to user passwords.

Blackboard Configuration File

The following parameters from the `bb-config.properties` file are covered by the Secure User Password Storage scheme immediately upon upgrade or new installation.

Note: System Administrators that previously used the configuration file as a location to record and reference passwords will no longer be able to do this since passwords will now be securely stored at rest.

No other configuration file changes are related to this Secure User Password Storage feature since this feature only covers credentials related to user passwords.

- antargs.default.users.administrator.password
- antargs.default.users.guest.password
- antargs.default.users.integration.password
- antargs.default.users.rootadmin.password

For customers upgrading from a version of Blackboard Learn prior to Release 9.1 Service Pack 12, the following parameters have been removed from the `bb-config.properties` file:

- antargs.default.users.administrator.password.md5
- antargs.default.users.guest.password.md5
- antargs.default.users.integration.password.md5
- antargs.default.users.rootadmin.password.md5

Database Changes to Support Secure User Password Storage

Secure User Password Storage uses pre-existing database tables. The password field has been expanded to accommodate the larger password hashes.

Background Jobs

There are no background Jobs associated with this security control.

Pre-existing user passwords are automatically migrated to the secure user password storage scheme upon successful authentication against the previous user password storage scheme.
New passwords automatically user the default secure user password storage scheme.

Security Audit Logging

Blackboard recommends that you monitor activity related to this security control.

Log events are part of Standard Security Event Codes. See Audit and Accountability for more information.

Log Location

Note: In an upcoming release, this log will be migrated to a central log file.

```
Blackboard_Home/logs/bb-security-authentication-log.txt
```

Event Codes

A severity of 0 is informational, 2 is a low alert, and 8 is a high alert.

Event Code	Severity	Definition
28	0	User Password Migrated to Default Secure User Password Storage Scheme.

Example Log Entry

```
timestamp=Aug 08 2008 08:08:08.888
EDT|app_vend=blackboard|app_name=learn|app_ver=9.1.120113.0|evt_code=2
8|evt_name=user password storage
migration|sev=0|cat=authentication|outcome=success|dhost=appsec-
demo.pd.local|src_ip=10.100.100.100|suid=13286|suser=securitystudent01
|session_id=6|msg=User password storage hash migrated
successfully.|http_useragent=Mozilla/5.0 (Macintosh; Intel Mac OS X
10_6_8) AppleWebKit/537.22 (KHTML, like Gecko) Chrome/25.0.1364.152
Safari/537.22|act= |request=/webapps/login/
```
