CakePHP SOS Fund Audit Fix Log

Identified Vulnerabilities

001: Mass Assignment Allowed by Default (High)

The code that generates entities has been updated to generate whitelists of fields, in https://github.com/cakephp/bake/pull/359 (released in cakephp/bake 1.4.2). We hope this makes the attributes that are mass-assignable more visible. We are not able to throw exceptions when additional attributes are included in POST data as this would cause a significant break in compatibility. In a future release we will explore additional ways to mitigate mass-assignment.

VERIFIED

003: Unsafe HTML Templates By Default (Medium)

Not fixed as our default templating engine does not have a way to enable auto-escaping in a global way. In the next major release we plan on adopting Twig (https://twig.symfony.com/) as our default templating engine which does offer auto-escaping.

VERIFIED

004: Multiple Html Helper Methods Do Not Escape URLs (Medium)

Fixed in https://github.com/cakephp/cakephp/pull/11092 Released in 3.5.1

NOT VERIFIED - There is another conditional in the assetUrl() function that can be matched to avoid URL sanitation: https://github.com/cakephp/cakephp/blob/0c88f6365f85e0659ff6cf571a3b709077fc11e9/src/View/Helper/UrlHelper.php#L161-L163.

Fixed in https://github.com/cakephp/cakephp/pull/11430

VERIFIED

005: HTML Helpers Do Not Escape Attribute Keys (Medium)

Fixed in https://github.com/cakephp/cakephp/pull/11092 Released in 3.5.1

VERIFIED

015: Incorrect X-Forwarded-For Header Parsing Allows IP Spoofing (Medium)

Fixed in https://github.com/cakephp/cakephp/pull/11093 Released in 3.5.1

VERIFIED

018: XML Entity Expansion Denial of Service (Medium)

Fixed in https://github.com/cakephp/cakephp/pull/11094 Released in 3.5.1

VERIFIED

009: randomBytes Returns Insecure Random Numbers (Low)

Fixed in https://github.com/cakephp/cakephp/pull/11099 To be released in 3.6.0 (currently available in 3.next in github). The addition of the exception was moved to a minor release as it could potentially cause unexpected errors for existing applications.

VERIFIED

010: Comment Incorrectly Advertises Mitigation for User Enumeration Timing Attack (Low)

Fixed in https://github.com/cakephp/cakephp/pull/11095 Released in 3.5.1

VERIFIED

012: Digest Auth Uses Non-Constant-Time Comparisons (Low)

Fixed in https://github.com/cakephp/cakephp/pull/11096 Released in 3.5.1

VERIFIED

014: Tutorial Application Allows Path Traversal in Pages Controller (Low)

Fixed in https://github.com/cakephp/bookmarker-tutorial/commit/b972831eb344dd9fedacea87e7bfd0e11dd23f82 This issue was already fixed in the application skeleton, but the bookmarker tutorial application had fallen behind.

VERIFIED

016: AutoLink Functions Use Predictable and Collision-Prone Hashes (Low)

Fixed in https://github.com/cakephp/cakephp/pull/11102 Released in 3.5.1

VERIFIED

019: Insecure Transport Encryption Protocols Supported (Low)

Fixed in https://github.com/cakephp/cakephp/pull/11338 To be released in 3.5.5

VERIFIED

020: Form Validation Tokens are not Associated With Users (Low)

Fixed in https://github.com/cakephp/cakephp/pull/11101 To be released in 3.6.0. This was moved out to the next minor release as changing the token format would cause applications to fail all token validation for forms that were generated on older versions. This potential breakage to application code is not something we felt belonged in patch release.

VERIFIED

021: Form Validation Tokens Are Vulnerable to Potential Hash Collisions (Low)

Fixed in https://github.com/cakephp/cakephp/pull/11101 To be released in 3.6.0. See 020 for context.

VERIFIED

022: Asset Middleware Can Serve Dot Files (Low)

Fixed in https://github.com/cakephp/cakephp/pull/11100 To be released in 3.5.1

VERIFIED

Miscellaneous Issues

002: Setters of Entity Attributes are not Always Called (Informational)

Documentation updated in https://github.com/cakephp/cakephp/pull/11117

VERIFIED

006: Insecure Default Hashing Algorithm (Informational)

Unfixed right now. Changing the default hash type is a risky change that will potentially break existing applications. We'll be changing the default to sha256 in 4.0.0.

007; CA Bundle Includes Untrustable CAs (Informational)

Fixed in https://github.com/cakephp/cakephp/pull/11104 Released in 3.5.1. We'll be updating the CA bundle in each minor release going forward.

VERIFIED

008: Insecure UUID Function (Informational)

Fixed in https://github.com/cakephp/cakephp/pull/11142 Released in 3.5.2. This fix is conditional on the environment having a secure random integer source.

VERIFIED

011: Digest Auth Uses MD5 Algorithm To Construct Nonces (Informational)

Fixed in https://github.com/cakephp/cakephp/pull/11103 Released in 3.5.1

VERIFIED