

Instantiation

hash

needs_rehash

verify

Bcrypt

The Bcrypt plugin is a secure and lightweight password hashing library.

Namespace: `\`

File location: `lib/bcrypt.php`

Notice: This plugin uses BLOWFISH to hash your passwords, which needs at least PHP version 5.3.7. Keep in mind to implement alternative hashing methods, if you aim to support lower versions as well (F3 itself requires 5.4 though).

Instantiation

```
$crypt = \Bcrypt::instance();
```

hash

Generate bcrypt hash of string

```
string|FALSE hash ( string $pw [, string $salt = NULL [, int $cost = 10 ]] )
```

If provided, the `$salt` parameter must be at least 22 alphanumeric characters.

The `$cost` parameter triggers the iteration count for the underlying Blowfish-based hashing algorithm and must be in range `04-31`.

needs_rehash

Check if password is still strong enough

```
bool needs_rehash ( string $hash [, int $cost = 10 ] )
```

If you decide to move to stronger passwords, you can check if the password hash will meet that `$cost` requirement. In case it's too weak, you could inform the user to choose a stronger one.

verify

Verify password against hash using timing attack resistant approach

```
bool verify ( string $pw, string $hash )
```