PasswordVerify

> **Note:** Using **passwordHash** is the recommended way of storing passwords.

This function verifies whether a password matches a password hash.

> **Warning:** It is strongly recommended to use the async version of the function (i.e. provide a callback function). Otherwise, you will experience short freezes due to the slow nature of the bcrypt algorithm

Syntax

```
bool passwordVerify ( string password, string hash [, table options, function callback ] )
```

Required Arguments

- **password:** The password to check.
- **hash:** A supported hash (see passwordHash). Note that only the prefix *$2y$* is supported for type bcrypt (older prefixes can cause security issues).

Optional Arguments

- **options:** advanced options
  - **insecureBcrypt:** If set to *true*, you can use the *$2a$* prefix for bcrypt hashes as well. **It is strongly not recommended to use it though, because the underlying implementation has a bug that leads to such hashes being relatively easy to crack.** This bug was fixed for *$2y$*.

- **callback:** providing a callback will run this function asynchronously, the arguments to the callback are the same as the returned values below.

Returns

Returns true if the password matches the hash. Returns false if the password does not match, or if an unknown hash was passed. If a callback was provided, the aforementioned values are arguments to the callback, and this function will always return *true*.