* [Welcome to CodeIgniter](http://docs.google.com/welcome.html)
* [Installation Instructions](http://docs.google.com/installation/index.html)
  + [Downloading CodeIgniter](http://docs.google.com/installation/downloads.html)
  + [Installation Instructions](http://docs.google.com/installation/index.html)
  + [Upgrading From a Previous Version](http://docs.google.com/installation/upgrading.html)
  + [Troubleshooting](http://docs.google.com/installation/troubleshooting.html)
* [CodeIgniter Overview](http://docs.google.com/overview/index.html)
  + [Getting Started](http://docs.google.com/overview/getting_started.html)
  + [CodeIgniter at a Glance](http://docs.google.com/overview/at_a_glance.html)
  + [Supported Features](http://docs.google.com/overview/features.html)
  + [Application Flow Chart](http://docs.google.com/overview/appflow.html)
  + [Model-View-Controller](http://docs.google.com/overview/mvc.html)
  + [Architectural Goals](http://docs.google.com/overview/goals.html)
* [Tutorial](http://docs.google.com/tutorial/index.html)
  + [Static pages](http://docs.google.com/tutorial/static_pages.html)
  + [News section](http://docs.google.com/tutorial/news_section.html)
  + [Create news items](http://docs.google.com/tutorial/create_news_items.html)
  + [Conclusion](http://docs.google.com/tutorial/conclusion.html)
* [Contributing to CodeIgniter](http://docs.google.com/contributing/index.html)
  + [Writing CodeIgniter Documentation](http://docs.google.com/documentation/index.html)
  + [Developer’s Certificate of Origin 1.1](http://docs.google.com/DCO.html)
* [General Topics](http://docs.google.com/index.html)
  + [CodeIgniter URLs](http://docs.google.com/urls.html)
  + [Controllers](http://docs.google.com/controllers.html)
  + [Reserved Names](http://docs.google.com/reserved_names.html)
  + [Views](http://docs.google.com/views.html)
  + [Models](http://docs.google.com/models.html)
  + [Helpers](http://docs.google.com/helpers.html)
  + [Using CodeIgniter Libraries](http://docs.google.com/libraries.html)
  + [Creating Libraries](http://docs.google.com/creating_libraries.html)
  + [Using CodeIgniter Drivers](http://docs.google.com/drivers.html)
  + [Creating Drivers](http://docs.google.com/creating_drivers.html)
  + [Creating Core System Classes](http://docs.google.com/core_classes.html)
  + [Creating Ancillary Classes](http://docs.google.com/ancillary_classes.html)
  + [Hooks - Extending the Framework Core](http://docs.google.com/hooks.html)
  + [Auto-loading Resources](http://docs.google.com/autoloader.html)
  + [Common Functions](http://docs.google.com/common_functions.html)
  + [Compatibility Functions](http://docs.google.com/compatibility_functions.html)
  + [URI Routing](http://docs.google.com/routing.html)
  + [Error Handling](http://docs.google.com/errors.html)
  + [Caching](http://docs.google.com/caching.html)
  + [Profiling Your Application](http://docs.google.com/profiling.html)
  + [Running via the CLI](http://docs.google.com/cli.html)
  + [Managing your Applications](http://docs.google.com/managing_apps.html)
  + [Handling Multiple Environments](http://docs.google.com/environments.html)
  + [Alternate PHP Syntax for View Files](http://docs.google.com/alternative_php.html)
  + Security
  + [PHP Style Guide](http://docs.google.com/styleguide.html)
* [Libraries](http://docs.google.com/libraries/index.html)
  + [Benchmarking Class](http://docs.google.com/libraries/benchmark.html)
  + [Caching Driver](http://docs.google.com/libraries/caching.html)
  + [Calendaring Class](http://docs.google.com/libraries/calendar.html)
  + [Shopping Cart Class](http://docs.google.com/libraries/cart.html)
  + [Config Class](http://docs.google.com/libraries/config.html)
  + [Email Class](http://docs.google.com/libraries/email.html)
  + [Encrypt Class](http://docs.google.com/libraries/encrypt.html)
  + [Encryption Library](http://docs.google.com/libraries/encryption.html)
  + [File Uploading Class](http://docs.google.com/libraries/file_uploading.html)
  + [Form Validation](http://docs.google.com/libraries/form_validation.html)
  + [FTP Class](http://docs.google.com/libraries/ftp.html)
  + [Image Manipulation Class](http://docs.google.com/libraries/image_lib.html)
  + [Input Class](http://docs.google.com/libraries/input.html)
  + [Javascript Class](http://docs.google.com/libraries/javascript.html)
  + [Language Class](http://docs.google.com/libraries/language.html)
  + [Loader Class](http://docs.google.com/libraries/loader.html)
  + [Migrations Class](http://docs.google.com/libraries/migration.html)
  + [Output Class](http://docs.google.com/libraries/output.html)
  + [Pagination Class](http://docs.google.com/libraries/pagination.html)
  + [Template Parser Class](http://docs.google.com/libraries/parser.html)
  + [Security Class](http://docs.google.com/libraries/security.html)
  + [Session Library](http://docs.google.com/libraries/sessions.html)
  + [HTML Table Class](http://docs.google.com/libraries/table.html)
  + [Trackback Class](http://docs.google.com/libraries/trackback.html)
  + [Typography Class](http://docs.google.com/libraries/typography.html)
  + [Unit Testing Class](http://docs.google.com/libraries/unit_testing.html)
  + [URI Class](http://docs.google.com/libraries/uri.html)
  + [User Agent Class](http://docs.google.com/libraries/user_agent.html)
  + [XML-RPC and XML-RPC Server Classes](http://docs.google.com/libraries/xmlrpc.html)
  + [Zip Encoding Class](http://docs.google.com/libraries/zip.html)
* [Database Reference](http://docs.google.com/database/index.html)
  + [Quick Start: Usage Examples](http://docs.google.com/database/examples.html)
  + [Database Configuration](http://docs.google.com/database/configuration.html)
  + [Connecting to a Database](http://docs.google.com/database/connecting.html)
  + [Running Queries](http://docs.google.com/database/queries.html)
  + [Generating Query Results](http://docs.google.com/database/results.html)
  + [Query Helper Functions](http://docs.google.com/database/helpers.html)
  + [Query Builder Class](http://docs.google.com/database/query_builder.html)
  + [Transactions](http://docs.google.com/database/transactions.html)
  + [Getting MetaData](http://docs.google.com/database/metadata.html)
  + [Custom Function Calls](http://docs.google.com/database/call_function.html)
  + [Query Caching](http://docs.google.com/database/caching.html)
  + [Database Manipulation with Database Forge](http://docs.google.com/database/forge.html)
  + [Database Utilities Class](http://docs.google.com/database/utilities.html)
  + [Database Driver Reference](http://docs.google.com/database/db_driver_reference.html)
* [Helpers](http://docs.google.com/helpers/index.html)
  + [Array Helper](http://docs.google.com/helpers/array_helper.html)
  + [CAPTCHA Helper](http://docs.google.com/helpers/captcha_helper.html)
  + [Cookie Helper](http://docs.google.com/helpers/cookie_helper.html)
  + [Date Helper](http://docs.google.com/helpers/date_helper.html)
  + [Directory Helper](http://docs.google.com/helpers/directory_helper.html)
  + [Download Helper](http://docs.google.com/helpers/download_helper.html)
  + [Email Helper](http://docs.google.com/helpers/email_helper.html)
  + [File Helper](http://docs.google.com/helpers/file_helper.html)
  + [Form Helper](http://docs.google.com/helpers/form_helper.html)
  + [HTML Helper](http://docs.google.com/helpers/html_helper.html)
  + [Inflector Helper](http://docs.google.com/helpers/inflector_helper.html)
  + [Language Helper](http://docs.google.com/helpers/language_helper.html)
  + [Number Helper](http://docs.google.com/helpers/number_helper.html)
  + [Path Helper](http://docs.google.com/helpers/path_helper.html)
  + [Security Helper](http://docs.google.com/helpers/security_helper.html)
  + [Smiley Helper](http://docs.google.com/helpers/smiley_helper.html)
  + [String Helper](http://docs.google.com/helpers/string_helper.html)
  + [Text Helper](http://docs.google.com/helpers/text_helper.html)
  + [Typography Helper](http://docs.google.com/helpers/typography_helper.html)
  + [URL Helper](http://docs.google.com/helpers/url_helper.html)
  + [XML Helper](http://docs.google.com/helpers/xml_helper.html)

Toggle Table of Contents

[CodeIgniter](http://docs.google.com/index.html)

* [Welcome to CodeIgniter](http://docs.google.com/welcome.html)
* [Installation Instructions](http://docs.google.com/installation/index.html)
  + [Downloading CodeIgniter](http://docs.google.com/installation/downloads.html)
  + [Installation Instructions](http://docs.google.com/installation/index.html)
  + [Upgrading From a Previous Version](http://docs.google.com/installation/upgrading.html)
  + [Troubleshooting](http://docs.google.com/installation/troubleshooting.html)
* [CodeIgniter Overview](http://docs.google.com/overview/index.html)
  + [Getting Started](http://docs.google.com/overview/getting_started.html)
  + [CodeIgniter at a Glance](http://docs.google.com/overview/at_a_glance.html)
  + [Supported Features](http://docs.google.com/overview/features.html)
  + [Application Flow Chart](http://docs.google.com/overview/appflow.html)
  + [Model-View-Controller](http://docs.google.com/overview/mvc.html)
  + [Architectural Goals](http://docs.google.com/overview/goals.html)
* [Tutorial](http://docs.google.com/tutorial/index.html)
  + [Static pages](http://docs.google.com/tutorial/static_pages.html)
  + [News section](http://docs.google.com/tutorial/news_section.html)
  + [Create news items](http://docs.google.com/tutorial/create_news_items.html)
  + [Conclusion](http://docs.google.com/tutorial/conclusion.html)
* [Contributing to CodeIgniter](http://docs.google.com/contributing/index.html)
  + [Writing CodeIgniter Documentation](http://docs.google.com/documentation/index.html)
  + [Developer’s Certificate of Origin 1.1](http://docs.google.com/DCO.html)
* [General Topics](http://docs.google.com/index.html)
  + [CodeIgniter URLs](http://docs.google.com/urls.html)
  + [Controllers](http://docs.google.com/controllers.html)
  + [Reserved Names](http://docs.google.com/reserved_names.html)
  + [Views](http://docs.google.com/views.html)
  + [Models](http://docs.google.com/models.html)
  + [Helpers](http://docs.google.com/helpers.html)
  + [Using CodeIgniter Libraries](http://docs.google.com/libraries.html)
  + [Creating Libraries](http://docs.google.com/creating_libraries.html)
  + [Using CodeIgniter Drivers](http://docs.google.com/drivers.html)
  + [Creating Drivers](http://docs.google.com/creating_drivers.html)
  + [Creating Core System Classes](http://docs.google.com/core_classes.html)
  + [Creating Ancillary Classes](http://docs.google.com/ancillary_classes.html)
  + [Hooks - Extending the Framework Core](http://docs.google.com/hooks.html)
  + [Auto-loading Resources](http://docs.google.com/autoloader.html)
  + [Common Functions](http://docs.google.com/common_functions.html)
  + [Compatibility Functions](http://docs.google.com/compatibility_functions.html)
  + [URI Routing](http://docs.google.com/routing.html)
  + [Error Handling](http://docs.google.com/errors.html)
  + [Caching](http://docs.google.com/caching.html)
  + [Profiling Your Application](http://docs.google.com/profiling.html)
  + [Running via the CLI](http://docs.google.com/cli.html)
  + [Managing your Applications](http://docs.google.com/managing_apps.html)
  + [Handling Multiple Environments](http://docs.google.com/environments.html)
  + [Alternate PHP Syntax for View Files](http://docs.google.com/alternative_php.html)
  + Security
  + [PHP Style Guide](http://docs.google.com/styleguide.html)
* [Libraries](http://docs.google.com/libraries/index.html)
  + [Benchmarking Class](http://docs.google.com/libraries/benchmark.html)
  + [Caching Driver](http://docs.google.com/libraries/caching.html)
  + [Calendaring Class](http://docs.google.com/libraries/calendar.html)
  + [Shopping Cart Class](http://docs.google.com/libraries/cart.html)
  + [Config Class](http://docs.google.com/libraries/config.html)
  + [Email Class](http://docs.google.com/libraries/email.html)
  + [Encrypt Class](http://docs.google.com/libraries/encrypt.html)
  + [Encryption Library](http://docs.google.com/libraries/encryption.html)
  + [File Uploading Class](http://docs.google.com/libraries/file_uploading.html)
  + [Form Validation](http://docs.google.com/libraries/form_validation.html)
  + [FTP Class](http://docs.google.com/libraries/ftp.html)
  + [Image Manipulation Class](http://docs.google.com/libraries/image_lib.html)
  + [Input Class](http://docs.google.com/libraries/input.html)
  + [Javascript Class](http://docs.google.com/libraries/javascript.html)
  + [Language Class](http://docs.google.com/libraries/language.html)
  + [Loader Class](http://docs.google.com/libraries/loader.html)
  + [Migrations Class](http://docs.google.com/libraries/migration.html)
  + [Output Class](http://docs.google.com/libraries/output.html)
  + [Pagination Class](http://docs.google.com/libraries/pagination.html)
  + [Template Parser Class](http://docs.google.com/libraries/parser.html)
  + [Security Class](http://docs.google.com/libraries/security.html)
  + [Session Library](http://docs.google.com/libraries/sessions.html)
  + [HTML Table Class](http://docs.google.com/libraries/table.html)
  + [Trackback Class](http://docs.google.com/libraries/trackback.html)
  + [Typography Class](http://docs.google.com/libraries/typography.html)
  + [Unit Testing Class](http://docs.google.com/libraries/unit_testing.html)
  + [URI Class](http://docs.google.com/libraries/uri.html)
  + [User Agent Class](http://docs.google.com/libraries/user_agent.html)
  + [XML-RPC and XML-RPC Server Classes](http://docs.google.com/libraries/xmlrpc.html)
  + [Zip Encoding Class](http://docs.google.com/libraries/zip.html)
* [Database Reference](http://docs.google.com/database/index.html)
  + [Quick Start: Usage Examples](http://docs.google.com/database/examples.html)
  + [Database Configuration](http://docs.google.com/database/configuration.html)
  + [Connecting to a Database](http://docs.google.com/database/connecting.html)
  + [Running Queries](http://docs.google.com/database/queries.html)
  + [Generating Query Results](http://docs.google.com/database/results.html)
  + [Query Helper Functions](http://docs.google.com/database/helpers.html)
  + [Query Builder Class](http://docs.google.com/database/query_builder.html)
  + [Transactions](http://docs.google.com/database/transactions.html)
  + [Getting MetaData](http://docs.google.com/database/metadata.html)
  + [Custom Function Calls](http://docs.google.com/database/call_function.html)
  + [Query Caching](http://docs.google.com/database/caching.html)
  + [Database Manipulation with Database Forge](http://docs.google.com/database/forge.html)
  + [Database Utilities Class](http://docs.google.com/database/utilities.html)
  + [Database Driver Reference](http://docs.google.com/database/db_driver_reference.html)
* [Helpers](http://docs.google.com/helpers/index.html)
  + [Array Helper](http://docs.google.com/helpers/array_helper.html)
  + [CAPTCHA Helper](http://docs.google.com/helpers/captcha_helper.html)
  + [Cookie Helper](http://docs.google.com/helpers/cookie_helper.html)
  + [Date Helper](http://docs.google.com/helpers/date_helper.html)
  + [Directory Helper](http://docs.google.com/helpers/directory_helper.html)
  + [Download Helper](http://docs.google.com/helpers/download_helper.html)
  + [Email Helper](http://docs.google.com/helpers/email_helper.html)
  + [File Helper](http://docs.google.com/helpers/file_helper.html)
  + [Form Helper](http://docs.google.com/helpers/form_helper.html)
  + [HTML Helper](http://docs.google.com/helpers/html_helper.html)
  + [Inflector Helper](http://docs.google.com/helpers/inflector_helper.html)
  + [Language Helper](http://docs.google.com/helpers/language_helper.html)
  + [Number Helper](http://docs.google.com/helpers/number_helper.html)
  + [Path Helper](http://docs.google.com/helpers/path_helper.html)
  + [Security Helper](http://docs.google.com/helpers/security_helper.html)
  + [Smiley Helper](http://docs.google.com/helpers/smiley_helper.html)
  + [String Helper](http://docs.google.com/helpers/string_helper.html)
  + [Text Helper](http://docs.google.com/helpers/text_helper.html)
  + [Typography Helper](http://docs.google.com/helpers/typography_helper.html)
  + [URL Helper](http://docs.google.com/helpers/url_helper.html)
  + [XML Helper](http://docs.google.com/helpers/xml_helper.html)

[CodeIgniter](http://docs.google.com/index.html)

* [Docs](http://docs.google.com/index.html) »
* [General Topics](http://docs.google.com/index.html) »
* Security

classic layout

Security[**¶**](#gjdgxs)

This page describes some “best practices” regarding web security, and details CodeIgniter’s internal security features.

Note

If you came here looking for a security contact, please refer to our Contribution Guide <../contributing/index>.

URI Security[**¶**](#30j0zll)

CodeIgniter is fairly restrictive regarding which characters it allows in your URI strings in order to help minimize the possibility that malicious data can be passed to your application. URIs may only contain the following:

* Alpha-numeric text (latin characters only)
* Tilde: ~
* Percent sign: %
* Period: .
* Colon: :
* Underscore: \_
* Dash: -
* Space

Register\_globals[**¶**](#1fob9te)

During system initialization all global variables that are found to exist in the $\_GET, $\_POST, $\_REQUEST and $\_COOKIE are unset.

The unsetting routine is effectively the same as *register\_globals = off*.

display\_errors[**¶**](#3znysh7)

In production environments, it is typically desirable to “disable” PHP’s error reporting by setting the internal *display\_errors* flag to a value of 0. This disables native PHP errors from being rendered as output, which may potentially contain sensitive information.

Setting CodeIgniter’s **ENVIRONMENT** constant in index.php to a value of **‘production’** will turn off these errors. In development mode, it is recommended that a value of ‘development’ is used. More information about differentiating between environments can be found on the [*Handling Environments*](http://docs.google.com/environments.html) page.

magic\_quotes\_runtime[**¶**](#2et92p0)

The *magic\_quotes\_runtime* directive is turned off during system initialization so that you don’t have to remove slashes when retrieving data from your database.

Best Practices[**¶**](#tyjcwt)

Before accepting any data into your application, whether it be POST data from a form submission, COOKIE data, URI data, XML-RPC data, or even data from the SERVER array, you are encouraged to practice this three step approach:

1. Validate the data to ensure it conforms to the correct type, length, size, etc.
2. Filter the data as if it were tainted.
3. Escape the data before submitting it into your database or outputting it to a browser.

CodeIgniter provides the following functions and tips to assist you in this process:

XSS Filtering[**¶**](#3dy6vkm)

CodeIgniter comes with a Cross Site Scripting filter. This filter looks for commonly used techniques to embed malicious JavaScript into your data, or other types of code that attempt to hijack cookies or do other malicious things. The XSS Filter is described [*here*](http://docs.google.com/libraries/security.html).

Note

XSS filtering should *only be performed on output*. Filtering input data may modify the data in undesirable ways, including stripping special characters from passwords, which reduces security instead of improving it.

CSRF protection[**¶**](#1t3h5sf)

CSRF stands for Cross-Site Request Forgery, which is the process of an attacker tricking their victim into unknowingly submitting a request.

CodeIgniter provides CSRF protection out of the box, which will get automatically triggered for every non-GET HTTP request, but also needs you to create your submit forms in a certain way. This is explained in the [*Security Library*](http://docs.google.com/libraries/security.html) documentation.

Password handling[**¶**](#4d34og8)

It is *critical* that you handle passwords in your application properly.

Unfortunately, many developers don’t know how to do that, and the web is full of outdated or otherwise wrongful advices, which doesn’t help.

We would like to give you a list of combined do’s and don’ts to help you with that. Please read below.

* DO NOT store passwords in plain-text format.  
  Always **hash** your passwords.
* DO NOT use Base64 or similar encoding for storing passwords.  
  This is as good as storing them in plain-text. Really. Do **hashing**, not *encoding*.  
  Encoding, and encryption too, are two-way processes. Passwords are secrets that must only be known to their owner, and thus must work only in one direction. Hashing does that - there’s *no* un-hashing or de-hashing, but there is decoding and decryption.
* DO NOT use weak or broken hashing algorithms like MD5 or SHA1.  
  These algorithms are old, proven to be flawed, and not designed for password hashing in the first place.  
  Also, DON’T invent your own algorithms.  
  Only use strong password hashing algorithms like BCrypt, which is used in PHP’s own [Password Hashing](http://php.net/password) functions.  
  Please use them, even if you’re not running PHP 5.5+, CodeIgniter provides them for you.
* DO NOT ever display or send a password in plain-text format!  
  Even to the password’s owner, if you need a “Forgotten password” feature, just randomly generate a new, one-time (this is also important) password and send that instead.
* DO NOT put unnecessary limits on your users’ passwords.  
  If you’re using a hashing algorithm other than BCrypt (which has a limit of 72 characters), you should set a relatively high limit on password lengths in order to mitigate DoS attacks - say, 1024 characters.  
  Other than that however, there’s no point in forcing a rule that a password can only be up to a number of characters, or that it can’t contain a certain set of special characters.  
  Not only does this **reduce** security instead of improving it, but there’s literally no reason to do it. No technical limitations and no (practical) storage constraints apply once you’ve hashed them, none!

Validate input data[**¶**](#2s8eyo1)

CodeIgniter has a [*Form Validation Library*](http://docs.google.com/libraries/form_validation.html) that assists you in validating, filtering, and prepping your data.

Even if that doesn’t work for your use case however, be sure to always validate and sanitize all input data. For example, if you expect a numeric string for an input variable, you can check for that with is\_numeric() or ctype\_digit(). Always try to narrow down your checks to a certain pattern.

Have it in mind that this includes not only $\_POST and $\_GET variables, but also cookies, the user-agent string and basically *all data that is not created directly by your own code*.

Escape all data before database insertion[**¶**](#17dp8vu)

Never insert information into your database without escaping it. Please see the section that discusses [*database queries*](http://docs.google.com/database/queries.html) for more information.

Hide your files[**¶**](#3rdcrjn)

Another good security practice is to only leave your *index.php* and “assets” (e.g. .js, css and image files) under your server’s *webroot* directory (most commonly named “htdocs/”). These are the only files that you would need to be accessible from the web.

Allowing your visitors to see anything else would potentially allow them to access sensitive data, execute scripts, etc.

If you’re not allowed to do that, you can try using a .htaccess file to restrict access to those resources.

CodeIgniter will have an index.html file in all of its directories in an attempt to hide some of this data, but have it in mind that this is not enough to prevent a serious attacker.

[Next](http://docs.google.com/styleguide.html)   [Previous](http://docs.google.com/alternative_php.html)

© Copyright 2014 - 2016, British Columbia Institute of Technology. Last updated on Oct 28, 2016.

Built with [Sphinx](http://sphinx-doc.org/) using a [theme](https://github.com/snide/sphinx_rtd_theme) provided by [Read the Docs](https://readthedocs.org).