Kentico CMS security facts

Kentico
unlimited website possibilities

www.kentico.com

Preface

The document provides the reader an overview of how security is handled by Kentico CMS. It does not give a full list of all possibilities in the described topics. Instead, it focuses on the most common scenarios and gives the reader the whole picture from a broad perspective. To fully understand this document, basic knowledge of Kentico CMS is required.

The last part of the document introduces new features which will be part of the next version of Kentico CMS.

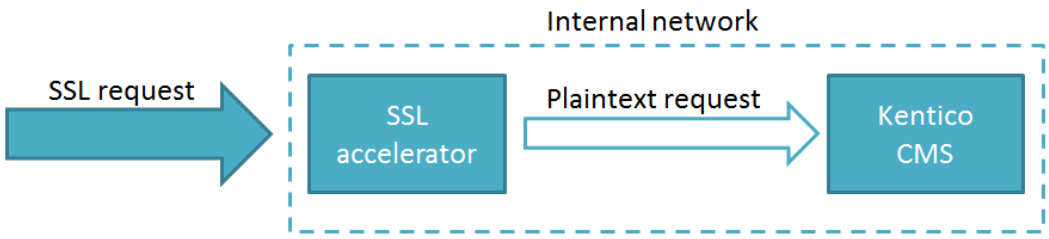
Elements which mitigate the risk of security vulnerabilities in Kentico CMS

Kentico software is continually integrating security elements into its SDLC (software development life cycle):

1. The design of each new module/functionality is reviewed by a security expert according to various security standards.
2. All developers and testers are continually trained in order to write secure code. Some of the used practices can be found in the Kentico CMS Security White Paper.
3. All our production code is reviewed by a Technical leader, the CTO and a Security expert (in this order).
4. All our functionality is verified by QA (quality assurance) tests. Among other things, these tests are focused on security.
5. Within the development department, there is one internal security team which periodically searches for security flaws in Kentico CMS code and its functionality.
6. Both the production and development versions of Kentico CMS are periodically scanned by an automatic Web application security tool. Currently, we are using Acunetix web vulnerability scanner for this purpose.
7. Every released version of Kentico CMS contains several new security features and enhancements (see the last chapter for details on what the next version of Kentico CMS will bring).
8. All security vulnerabilities found in production code are fixed within 7 days.

SSL support

Kentico CMS supports SSL (HTTPS) on both the live site and in the administration interface. SSL support can be set up for the whole system or only for certain parts. We also support SSL accelerators.



Picture 1: SSL accelerator scenario

Authentication

By default, Kentico CMS uses the ASP.NET Forms authentication mechanism. We built our own ASP.NET membership provider in order to give you the ability to use standard ASP.NET membership controls for sign up, log in and log out. Also, Kentico CMS offers authentication against Active directory (Windows authentication). You can even combine these two authentication types.

You can also use the following 3rd party services for authentication:

- Windows live ID
- Open ID
- Facebook connect
- LinkedIn

PASSWORDS IN THE KENTICO CMS DATABASE

Kentico CMS offers the following options for storing users' passwords in the database:

- Plain text (not recommended)
- Hashed in MD5
- Hashed in SHA1
- Hashed in SHA2
- Hashed in SHA2 with salt (recommended)

The recommended solution is to store data hashed in SHA2 with salt, this is also the default option.

There is also a need to store different types of passwords in Kentico CMS, for example the password of a SMTP server or a SharePoint server. These passwords must be retrievable, so they cannot be hashed. Instead of that, they are encrypted in the database using asymmetric cryptography.

PASSWORD POLICY

Kentico CMS provides the ability to force users to set up their password according to the following rules:

- Minimum length of the password.
- Minimum number of non-alphanumeric characters in the password.
- Passwords must match a certain format specified by a regular expression.

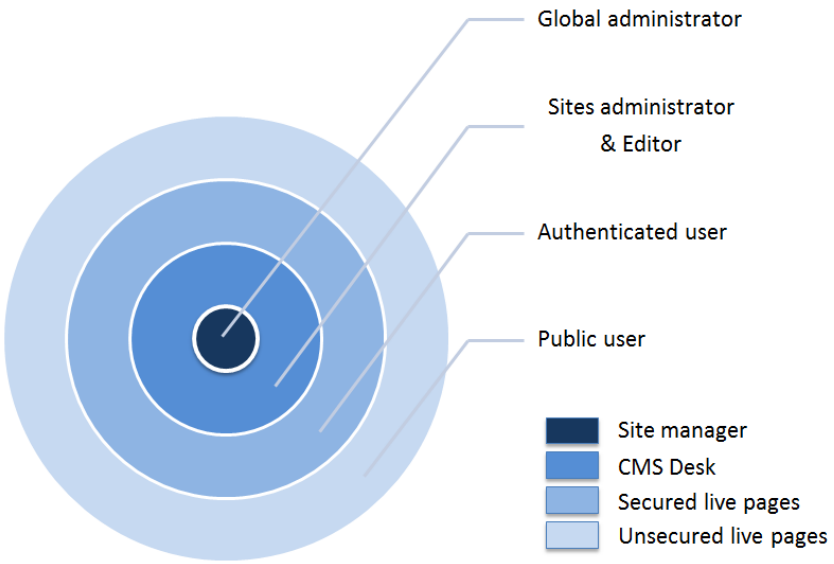
Authorization

Kentico CMS has three different user interfaces:

- **Live site** – Front end for site visitors.
- **CMS Desk** – Administration of one certain site. The place where content is edited.
- **Site manager** – Administration of the whole CMS platform. The place where sites are managed.

Kentico CMS divides users on the following levels:

- **Public user** – has permissions to see live unsecured resources (pages, documents, images …) on the live site, represents a site visitor who hasn't logged in.
- **Authenticated user** – a logged in site visitor, can see some secured resources on the live site (depending on assigned roles).
- **Editor** – has access to CMS Desk on the assigned sites.
- **Sites administrator** – have access to CMS Desk on all sites within the system. They can manage all objects of all sites but don't have access to Site Manager.
- **Global administrator** – have access to Site manager. User with all permissions.



Picture 2: User levels

The Public user, Sites administrator and Global administrator user types have permissions determined by their user level. The other two types, Authenticated users and Editors, are more flexible and their permissions are determined by their roles.

USER ROLES

Each user can belong to any number of roles, their relationship is N:M. The roles are related N:1 to sites, every role belongs to a certain site.

PERMISSIONS & UI ELEMENTS

Permissions for the whole system are manageable in one place in the Administration interface. They are role based – you cannot assign specific permissions to a user directly, you always need to assign the user to a role and then give the role certain permission(s). There are two types of permissions:

- **Functional (permissions)** – Permission check is done after the user performs a given action. If the action is not permitted, an error message is shown in the interface.
- **Visual (UI elements)** – Permission check is done during the page rendering. If a certain action is not available, the corresponding action button/link is not rendered and the user doesn't see it in the interface.

There are two standard permissions – read and modify (manage). Also, many modules have their own specific set of permissions for better granularity or for better handling of special scenarios. For example, the Users module has the special permission "Manage user roles" which allows a given role to add or remove a user from/to a role.

There are also modules, for example the Forum module, where you can specify a special set of permissions directly in the module's configuration and even from the live site. It is assumed that these modules will be managed directly by Authenticated users who don't have access to the Administration interface (CMS Desk).

DOCUMENT ACLS

Every document (page) created in Kentico CMS has its own ACL (access control list). In this list you can specify which roles are permitted to read, modify, create, delete or destroy (delete permanently) the current document or its child documents.

Protection

There are lots of features in Kentico CMS which help an administrator protect the production site against various attacks. First of all, you can disable the whole administration interface for a production site. After that, even if the administration account is compromised, nobody can damage the site through the administration.

BANNED IPS

The Banned IPs module is useful when you want to prevent users with certain IP addresses from accessing or using your website in a certain way. This typically happens when a user posts offensive material on a website (e.g. on a forum), harasses site members or behaves in some other unwanted way. IP banning can also be used to restrict access to your

websites from certain areas of the world. These bans can be set either for individual websites or globally for all websites in the system.

E-MAIL CONFIRMATION OF USER ACTIONS

Certain actions, such as a password reset or newsletter subscription, need approval via the given user's e-mail. This prevents unauthorized people from performing these actions and as a side effect, it informs the victim about potential abuse.

FLOOD PROTECTION

This feature prevents users from sending too many messages in modules such as Forums or Message boards within a short period of time. You can specify the minimum interval during which users cannot send new messages.

EVENT LOG

Every exception/error in Kentico CMS is logged into the Kentico CMS event log. From this log, administrators can analyse what is happening when someone tries to attack their web site. Among other things, the following information can be found there:

- Successful and unsuccessful login into the system
- User password change
- Errors during SQL query execution (allows you to detect SQL injections)
- Access to non-existing pages
- Unauthorized manipulation with page parameters

CAPTCHA

Completely automated public Turing test to tell computers and humans apart (CAPTCHA) helps you distinguish between people and computer programs (bots/spiders). Kentico CMS offers two types of CAPTCHA tests. The first one is in the form of text rendered as an image which must be entered by the user. Unfortunately, this test can be forged through OCR technology. The second one is a logical CAPTCHA, which tests the user using easy math or logic problems.

URL HASHES

Almost every URL in Kentico CMS is protected by a special parameter in the URL – a hash. This hash is calculated from the given URL parameters and it ensures that the parameters are not changed by a user. If a given hash is not equal to the hash generated for the original URL parameters, the request is not processed.

New features and enhancements for Kentico CMS 7

In the next version of Kentico CMS, we are preparing several new features which make your web sites even more secure. The following list describes a few of them:

- **Invalid password attempts** – It will be possible to specify the maximum number of login attempts. If a user exceeds the specified number, their account will be locked.
- **Password expiration** – you will be able to specify an interval for which passwords will be valid. Then, a user will be forced to change the password.
- **Screen locking** – Similar feature to operation system lock. After a specified time interval, the active window locks and users will have to enter a valid password in order to work with the system again.
- **Ability to enforce password policy** - There will be a possibility to force users to change their password right after logging in. Otherwise, they will not be able to use the system.
- **Built in protection against Clickjacking** – Clickjacking is a relatively new kind of attack. This attack displays the victim's website in an iframe on the attacker's site.. Kentico CMS adds a special HTTP header to each page to ensure that the page cannot be rendered in an iframe on a different domain.
- **Autocomplete** – All log-in forms will not remember previous input values, the autocomplete feature in these from will be disabled by default.