Kentico 7 Security guide Home

This is the security guide for Kentico 7.0. Please continue to the Security guide - Introduction page or choose a page from the list below.

Space Index

Total number of pages: 60

0-9 ... 0	A ... 3	B ... 1	C ... 8	D ... 6	E ... 2
F ... 2	G ... 0	H ... 2	I ... 1	J ... 0	K ... 1
L ... 1	M ... 3	N ... 0	O ... 0	P ... 5	Q ... 1
R ... 2	S ... 15	T ... 1	U ... 1	V ... 0	W ... 1
X ... 1	Y ... 0	Z ... 0	!@#$ ... 0		

0-9

A

Page: Argument injection
Argument injection is a type of attack based on tampering with input parameters of a page. This can enable attackers to see data which they normally cannot see or to modify data which they normally cannot modify, via the user interface. Example of argumen

Page: Autocomplete deactivation
Autocomplete is a feature, which remembers submitted user names in login forms and also all words submitted through any forms in the system. In this topic though, we will focus only on the autocomplete functionality in login forms: image2013-7-29 8:32:27.

Page: Avoiding security vulnerabilities in code
In this section you will learn how to protect your system against various types of hacker and scripting attacks. @self

Recently Updated

Kentico 7 Security guide
Dec 21, 2015 • updated by J ana Pelclova

Security guide - Introduction
Sep 12, 2014 • updated by J ana Pelclova • view change

Kentico 7 Security guide Home
Sep 12, 2014 • updated by J ana Pelclova • view change

Kentico 7 Security guide Home
Mar 05, 2014 • updated by Anonymous • view change

Clickjacking
Mar 04, 2014 • updated by J ana Pelclova • view change

Forgotten password
Feb 07, 2014 • updated by David Beovský • view change

Special permissions
Feb 07, 2014 • updated by David Beovský • view change

Lightweight Directory Access Protocol (LDAP) injection
Nov 26, 2013 • updated by David Štula • view change

Creating custom error handling pages
Oct 15, 2013 • updated by J ana Pelclova • view change

Save.png
Oct 15, 2013 • attached by J ana Pelclova

Password strength policy and its enforcement
Oct 15, 2013 • updated by J ana Pelclova • view change

AddNewUICulture.png
Oct 15, 2013 • attached by J ana Pelclova

Disabling unnecessary modules and services and keeping the system up-to-date
Oct 14, 2013 • updated by J ana Pelclova • view change

Security checklist - deploying a website
Sep 20, 2013 • updated by J ana Pelclova • view change

Web.config file settings
Sep 20, 2013 • updated by J ana Pelclova • view change

B

Page: Banned IPs

IP banning prevents users with specified IP addresses from using your website. Kentico CMS provides these levels of IP address banning: Access to the website - users with the specified IP address cannot access the site at all. Login - users cannot log in

C

Page: Clickjacking

Clickjacking is a type of attack where the attacker tricks website users into clicking something different that what they see, thus performing an action that may, for example, reveal confidential data or have any other negative impact on the user. In a ty

Page: Command injection

Code injection in ASP.NET is not a well known issue. It is because in ASP.NET, code files are not inserted one into another dynamically (like in PHP). Programmers can only register controls in the web.config file or on a page. But dynamic code injection i

Page: Configuring e-mail confirmations

It is recommended to use all kinds of e-mail confirmations Kentico provides. The e-mail confirmations protect the users from being subscribed to mass e-mails or having their passwords changed without their knowledge. Password change confirmation You can a

Page: Configuring permissions securely

Permissions allow you to control access to the particular sections of the Kentico administration interface by users. To learn how the whole system works, continue through the following sections: Configuring permissions securely Configuring permissions sec

Page: Configuring SSL

The Secure Sockets Layer protocol is used to encrypt Internet communication. This is important for protecting privacy of your users and for safekeeping sensitive information that is being sent. If you do not protect the sensitive information on your websi

Page: Creating custom error handling pages

You can configure the system to display custom pages instead of standard error messages. Custom pages help reduce the inconvenience caused to visitors if they run into an error while browsing your website, and also improves the security of the site by hid

Page: Cross site request forgery (CSRF/XSRF)

A browser typically uses two ways of requesting web applications. It sends data via URL parameters where HTTP GET request is used and sends data via forms where HTTP POST is used. The application typically does some action, for example, inserts a new user

Page: Cross site scripting (XSS)

Cross site scripting happens when somebody (an attacker) inserts a malicious input into a form (for example, a piece of HTML code). Depending on what happens after that, we divide XSS attacks into these types: Persistent XSS - a web application (like an

D

Page: Deploying web applications to a secure environment
security-process-5.png @self

Page: Designing secure error messages
When designing error messages, you should always consider the level of information revealed to the user. If you reveal too much information, the user may be overwhelmed and confused. Moreover, malicious users may exploit this information to gain detailed

Page: Designing secure web applications
security-process-3.png @self

Page: Developing secure web applications
security-process-4.png @self

Page: Directory traversal
This type of attack is also known as path traversal. The main goal is to show content of a file or directory via an application. Applications read data from the file system in many cases. Paths to these files or directories are often taken from input. If

Page: Disabling unnecessary modules and services and keeping the system up-to-date
You should enable only those services, which your application needs. Otherwise, you provide more opportunities for attackers to infiltrate your system. Many services are installed by default, so you should take care to disable those you do not actually ne

E

Page: Enumeration
Enumeration, in terms of security, is a vulnerability, which enables a potential attacker to guess some hidden system information. There are many types of enumeration threats, but we will discuss only two of them in this topic: Enumeration Enumeration Use

Page: Excerpt macro
EMS requirement excerpt Features described on this page require the Kentico EMS license.

F

Page: Flood protection
Flood control is a form of spam prevention on forums and similar community services. It prevents the users from making posts to the forum in quick successions. The users usually have to wait for a short time period before making another post. This mechani

Page: Forgotten password
If users forget their password, they may retrieve or reset it, provided they have access to the email address specified for their account. A password may be recovered by submitting a request through one of the website's logon forms. By default, a forgott

G

H

Page: Handling error messages securely
Displaying information to the users in error messages is an important issue which you should pay attention to. Revealing some pieces of information (for example stack trace or debug data) can pose a security risk to your site, while not providing enough i

Page: Hiding the system information
You should always try to hide the information about the server and operating system you are using. When the attackers are not able to determine this information, it is much more difficult for them to find flaws in the system and exploit them. If attacker

I

Page: Invalid logon attempts
One of the most common threats to website security is stealing user accounts. To compromise an account, attackers use a simple method, which tries to guess the password for that account, either by combining different characters, or by selecting passwords

J

K

Home page: Kentico 7 Security guide Home
This is the security guide for Kentico 7.0. Please continue to the Security guide - Introduction page or choose a page from the list below.

L

Page: Lightweight Directory Access Protocol (LDAP) injection

LDAP is a protocol for accessing and modifying the directory services over TCP/IP. This protocol has many implementations. However, we will focus only on the Active Directory Lightweight Directory service in this topic, as it is used by Kentico. The LDAP

M

Page: Macros and security

Macros are an essential part of Kentico CMS. You can read more about them in the Macro expressions http://devnet.kentico.com/docs/devguide/index.html?macro_expressions_overview.htm chapter. This topic focuses on the security mechanisms and best practices

Page: Managing external authentication

External authentication services Kentico supports several external authentication methods out of the box. To use them on your site, you have to configure them first (click on respective links for instructions) and place a corresponding web part on a page

Page: Minimal secure configuration

Your web application should be run with the smallest set of rights that allow the application to function correctly. For example, a web application should NOT have access anywhere outside of the web application space. When attackers happen to find a flaw

N

O

P

Page: Password encryption in database

There are multiple different formats that can be used to store passwords in the database. They may be saved either in plain text or as the result of a security hash function. You can choose which option should be used in Site Manager -> Settings -> Securi

Page: Password expiration

With the available password settings in Site Manager -> Settings -> Security & Membership -> Passwords, you can set the passwords to expire after a specified amount of time. You can turn on password expiration with the Enable password expiration setting.

Page: Password strength policy and its enforcement

The system can be configured to use a password policy, which means that new passwords entered by users will be validated according to a certain set of requirements. Passwords that do not meet the specified conditions will be rejected. Configuring a passwo

Page: PCI compliance

PCI DSS The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements meant to ensure that companies involved in the process of card payment maintain a certain level of security to protect the cardholder data. It was designed by majo

Page: Preventing duplicate poll voting and content rating

When you include polls and content rating functionalities on your website, you usually want to assure, that each user can vote only once. This is very difficult or nearly impossible to achieve. You should keep in mind that there will always be users that

Q

Page: Query string hashing

Query strings in the URLs are useful and important in many ways, for example, in passing various values between pages or in retrieving data from the database. In some cases though, an unauthorized user could obtain sensitive data or harm the system by ent

R

Page: Restricting access to directories

It is recommended that you allow users to access only those directories they actually need. This means that you must forbid access to the chosen directories for all users that do not need them. This can be configured in the web.config file. This example f

Page: Restricting access to the CMSHelp directory

S

Page: Screen locking

When users, who are signed in to the Kentico administration interface, leave their workstations unattended, someone else can tamper with the system. For this reason, Kentico allows you to set up automatic screen locking. This feature locks the working are

Page: Secure coding recommendations

Kentico CMS comes with an online help reference that is available in most parts of the administration interface. Users can view it to learn contextspecific information about the current section of the application's interface. By default, any users (incl

In this section you will find information and recommendations on how to: Securely work with macros Protect query string parameters Securely handle error messages

Page: Securing and protecting the system

In this section you will learn how to set up your system, so that it is protected against spam bots, fraudsters and malicious users. @self

Page: Securing the Staging and REST web services

Kentico offers two services which provide communication and synchronization of content and objects between servers. Both services are disabled by default. You should turn the services on only if you know you will be needing them. You can enable Staging at

Page: Securing user accounts and passwords

Passwords are a critical part of any authentication process. Kentico CMS provides various passwordrelated features that you can leverage to achieve the level of security required by your website. These settings can be found in Site Manager -> Settings ->

Page: Security checklist - deploying a website

This is a security deployment checklist – things to do before you deploy your site to a live environment. Web.config: Check Description Details The debug mode is turned off to prevent sensitive information leakage. Web.config file settings Tracing is

Page: Security checklist - designing a website

This is a design checklist – facts you should consider before you begin developing your website. Security requirements Check Description I know how critical the application safety will be (whether it is a blog, corporate website, e-shop, bank applicatio

Page: Security checklist - developing a website

This is a design checklist – things you should keep in mind while developing websites. User inputs Check Description User inputs are checked for type, length and content. User inputs with arithmetic operations are checked and validated for minimum a

Page: Security checklists

In this section you can find lists of tasks, which we recommend you to perform in the given stages of development.

Page: Security guide - Introduction

Security is an important factor in web development process. Ideally, security should be addressed at the beginning, before you even start planning and designing your projects. Reality though, is more complicated, and in many projects, security issues are

Page: Session protection

We use sessions, because web is running on HTTP, which is a stateless protocol. However, in many web applications, we need to keep some state information, some context. This is the purpose of sessions. When a user opens a browser and navigates to some web

Page: Spam protection (CAPTCHA)

Kentico CMS allows you to protect your website from automated spam bots. You can secure all forms where users enter data, by requiring users to type a security code called CAPTCHA http://cs.wikipedia.org/wiki/CAPTCHA. You can use CAPTCHA to tell humans an

Page: Special permissions

	The purpose of special permissions in Kentico CMS is to prevent the privilege elevation attack. In this type of attack, a lower privilege user can gain access to functions only available for higher privilege user. For example, CMS editors with permissions Page: SQL injection SQL injection is a well known web application vulnerability. The attacker's aim is to execute his own SQL code on the victim's database through a web application. How can the attacker do that? The attack is similar to XSS. The attacker inserts a special s Page: SSL accelerator support In some scenarios, SSL decryption and encryption may not performed directly by your application's server. Instead, the decryption and encryption is performed via a reverse proxy, which is equipped with an SSL offload hardware (for example, an SSL accelera
T Page: The event log and security debug Event log The event log is a place in the administration interface, where events and activities of the system are recorded. You can find it in Site Manager -> Administration -> Event log. From the security point of view, the events logged into the event l	**U** Page: Unlocking an account A user account can be locked for one of the following reasons: The user's password expires. The user reaches the limit of invalid logon attempts. The following text describes how you can provide users with means to unlock their accounts. Password expired
V	**W** Page: Web.config file settings In this topic, you will find a list of the most important settings which can be configured in the web.config file. Authentication You can set the default authentication mode for your website using the mode attribute, which has these values: Windows, Forms
X Page: XPath injection The principle of XPath injection is very similar to SQL injection. The goal of the attack is very similar too. The only difference between these attacks is that XPath injection uses an XML file for data storage instead of a database. One way to get data f	**Y**
Z	**!@#$**