ireland
website design

JOOMLA SECURITY

by Oliver Hummel

ADDRESS

Unit 12D, Six Cross Roads Business
Park, Waterford City

CONTACT

Nicholas Butler
051-393524 | 089-4278112
info@irelandwebsitedesign.com

Contents

CONFIDENTIALITY INFORMATION

This material contained in our response and any material or information disclosed during discussions of the proposal represents the proprietary, confidential information pertaining to Ireland Website Design company services, methodologies and methods. Products and brand names are intellectual property and all rights reserved.

Introduction

This document gives you a detailed look into securing your Joomla website. The biggest vulnerability to Content Management System based websites are outdated versions of the plugin or the CMS itself. Always make sure to update these. We suggest to also install additional security plugins.

Plugin

The plugin we use is Akeeba Admin Tools Professional.
More information and download link can be found here:
http://extensions.joomla.org/extension/admin-tools

Akeeba Admin Tools

Installation

The installation is simple and works the same as every other plugin. Go to the Extension Manager (Extensions > Manage) and select the tab ‘Upload Package File’. Select the zip archive and click Upload & Install. After the installation the extension can be found under Components > Admin Tools. You then have to provide your Download key and a password. This password is an additional security layer. If somebody gets access to the backend they still can’t make changes to the plugin settings.

Web Application Firewall

This is the core security feature of the plugin. It blocks malicious input and prevents Brute Force Attacks on the backend. Here is how to configure it:

[optional]

If your office has a fixed IP address you can lock out everybody else from the Joomla backend. But remember that you can only gain access to your website from your office. To enable this feature add your IP to the Whitelist (Web Application Firewall > Administrator IP Whitelist).

Go to Web Application Firewall > Configure WAF. You find nine tabs where you can change settings. These are not all settings but those we consider important.

Basic Protection Features

<u>Allow administrator access only to IPs in Whitelist</u>
If you put your IP into the whitelist, set this to yes to lock out other IPs.
<u>Administrator secret URL parameter</u>
This option changes the default link to the backend. You can specify a secret parameter *x*. Then you need to go to *domain.com/administrator?x* to log in.
<u>Change administrator login directory</u>
This also changes the address to log in. Change it from the default */administrator* to something custom. But it might not be working on your server and Akeeba doesn’t provide support for it. Use with caution.

Active Request Filtering

SQLiShield protection against SQL injection attacks YES

Detects common SQL injection attacks against your site and blocks them.

Cross Site Scripting block (XSSShield) YES

Detects common cross-site scripting (XSS) attacks and blocks them.

Allow PHP tags in request NO

Set this to NO! Otherwise hackers might be able to execute PHP scripts.

XSS-safe request parameters LEAVE DEFAULT

Malicious User Agent block (MUAShield) YES

Blocks the ability to send PHP in the user agent string of the browser.

CSRF/Anti-spam form protection (CSRFShield) ADVANCED

Prevents spam on forms by adding a hidden input, spammers try to fill in.

Remote File Inclusion block (RFIShield) YES

Direct File Inclusion shield (DFIShield) YES

Uploads Scanner (Upload Shield) YES

All uploaded files are scanned for PHP code.

Anti-spam filtering based on Bad Words list

You need to input a list with words users must not use in forms if you want to enable this feature.

Joomla Feature Hardening Options

Disable editing backend users’ properties YES

Changing the user properties can only be done by the person who has the Akeeba Admin Tools password. This might not be neccessary for your site.

Treat failed logins as security exceptions YES

All failed logins are now logged.

Visual Fingerprinting Protection

Those settings try to hide that you are using Joomla and block template switching. The following settings can be applied:

Hide/customise generator meta tag YES

Generator tag COMPANY NAME [OR SOMETHING ELSE]

Block temp=foo system template switch YES

List of allowed tmpl= keywords LEAVE DEFAULT

Block template=foo site template switch YES

Allow site templates YES

Auto-ban Repeat Offenders

IP blocking of repeat offenders YES

Stops Brute Force Attacks by blocking the IP after several failed logins

Block after 5 ATTACKS IN 15 MINUTES

Block for this long 15 MINUTES

IP blacklisting of persistent offenders YES

Permanently blacklist IP after 5 AUTOMATIC IP BLOCKS

These are settings we recommend for your website. I should give you an additional layer of security. You can now save the settings and close the Web Application Firewall.

.htaccess Maker

Akeeba Admin Tools comes with the ability to create custom htaccess files. If your website is running on an Apache Webserver (most of them are), you can stop people from looking at certain files or directories. Even if you don’t need to block certain directories, these basic settings protect you from a few security risks:

Disable directory listing (recommended) YES

Very important, otherwise Apache shows all files in a directory if no index document is present.

Protect against common file injection attacks YES

Protects against exploits and malicious code execution on the server.

Disable PHP Easter Eggs YES

Tries to stop hackers from finding out which PHP version you are running.

Block access to configuration.php-dist and htaccess.txt YES

Those files are created after a Joomla installation and can be directly accessed from the web. They tell the user what Joomla version you use.

Protect against clickjacking YES

Reduce MIME type security risks YES

Prevents users from uploading executable files with IE9 and Chrome.

Reflected XSS prevention YES

Prevents the most common form of Cross Site Scripting Attacks where injected scripts are reflected off the webserver in error messages, search results or any message where form input is shown to the users.

Remove Apache and PHP version signature YES
Prevent content transformation YES
Prevent issues when trying to compress CSS/JavaScript in congested networks.
Block access from specific user agents YES
Akeeba provides a list of bad user agents that are used by spammers. You can also look for more up to date lists on the internet.

The settings below are mainly used for file and directory protection. Once you are done you can either save without creating a file, to store your configuration, or save it and create an htaccess file.

Helpful Tools

There are a few other helpful tools that are worth checking every once in a while.

Repair and optimise tables

This cleans your database by repairing tables. This process can take a bit of time.

Fix Permissions

Some plugins can change the file permissions and make them less secure. Directories should be set to 755 and files to 644. This tools does this automatically. This is how to decode those numbers:

1. Number: Permissions of the owner the files belong to
2. Number: Permissions of the groups the files belong to
3. Number: Permissions of everybody on the server

0: no permissions
4: read
5: read and execute
6: read and write
7: read, write and execute

Unit 12D, Six Cross
Roads Business Park,
Waterford 051-393524 | 089-4278112
www.irelandwebsitedesign.com
info@irelandwebsitedesign.com