AdminExile 2.3.6

Overview

AdminExile is a Joomla system plugin designed to secure access to the /administrator URL and prevent unauthorized access to the /administrator login form itself.

Installation

1. Download AdminExile from the RicheyWeb download page.
    - This page will remain unlinked, as the link may change in the future. Visit http://www.richeyweb.com (http://www.richeyweb.com) and use the search feature - search for "adminexile".
2. In Joomla /administrator, go to the "Extensions" menu, the "Manage" sub-menu, and the "Install" sub-menu.
3. Select the "Upload Package File" tab
4. Press the "Choose File" button to browse your system and locate the plugin file you downloaded
5. Press the "Upload & Install" button

At this point, the extension is installed but not enabled. If you enable it without configuration, it will work - but the URL keys will be default (well known) and not secure. Enabling without configuration is NOT recommended.

Configuration

Because this is a complex plugin, it has many options for configuration. Each configuration type is separated onto tabs within the plugin configuration and these tabs are addressed separately (but in order) within this documentation.

Plugin

This is the basic configuration tab (the initial tab displayed) when editing the plugin configuration. It is on this tab where the plugin can be published and unpublished. It is suggested to configure, save, then enable. Don't get ahead of yourself or you may need the "HELP" section (below) sooner than later.

The default options are as follows:

- URL Access Key: adminexile
- Use Key + Value: No
- Key Value: ROCKS
    - Not displayed unless "Use Key + Value" is set to Yes
- Allow Re-Entry: No
- Re-Entry Seconds: 60
    - Not displayed unless "Allow Re-Entry" is set to Yes
- Redirect URL: {HOME}
- 404 Template: described below

Another portion of this tab, above the configuration options is the "Your URL:" link. This is a live updated URL which reflects the currently configured options within this tab of the plugin. As you alter the key or key value, the display shows the new URL that will be active when the plugin is saved and activated. You can return at any time to the plugin configuration to retrieve the current /administrator URL.

URL parameters (variables) are restricted to a certain list of characters, and additionally - there are some characters which have a special meaning to Joomla. AdminExile actively monitors the input values of the key and key-value fields to ensure that an invalid character isn't entered. Don't bother typing these, as the plugin will not allow them to be used and will display this list to remind you. It's much easier to display the list of invalid characters, so they are presented here:

Invalid Characters

- SPACE- ( )
- QUOTE- "
- POUND- #
- DOLLAR- $
- PERCENT- %
- AMPERSAND- &
- PLUS- +
- COMMA- ,
- FORWARDSLASH- /
- COLON- :
- SEMICOLON- ;
- LESS THAN- <
- EQUALS- =
- GREATER THAN- >
- QUESTION- ?
- AT- @
- LEFT BRACKET- [
- BACKSLASH- \
- RIGHT BRACKET-]
- CARAT- ^
- GRAVE- `
- LEFT CURLY- {
- PIPE- |

- RIGHT CURLY- }
- TILDE- ~

URL Access Key

The default setting is "adminexile".

It is possible to use ONLY this configuration option. This is like adding a password to enter your gate before someone can approach your front door. They can't break in the door, if they can't get past the gate.

Passwords are notoriously easy to break. Give a machine some time and it will eventually break any password. A good rule of thumb is, your password should be longer than 8 characters. Any shorter and it can be broken in a matter of hours (minutes and seconds for the very shortest passwords).

There are numerous places for password advise online. Pick something you like, something longer than 8 characters, and please don't let it be "adminexile" (the default)

Use Key + Value

The default setting is "No".

It is suggested that you turn this to "Yes" and configure your own key value below. Enabling this option will reveal the Key Value configuration option.

Key Value

The default setting is "ROCKS".

Continuing with the gate password analogy used above, the key value is like hiding the keypad. Now not only must they know the correct code (the value) but they also must find the keypad to enter it (the URL Access

Key). This additional layer of complexity now requires the attackers to crack two related passwords simultaneously, making the time to crack astronomical.

Like the URL Access Key, the longer the better. Choose something longer than 8 characters and consult a guide to pick the best and most secure password.

Some have suggested that this feature is overkill - but can an attack really ever be dead enough? We think it should be killed just a little more - to be absolutely sure.

Allow Re-Entry

The default setting is "No".

It is suggested that you leave this setting as "No". When enabled, it allows a user to log out of /administrator and NOT be redirected away for a configurable number of seconds. In other words, when they log out, they're presented with the /administrator login form WITHOUT entering the key or the key+value.

This feature was added after a tremendous user demand for it. We believe it introduces an insecurity and should never be turned on.

Re-Entry Seconds

The default setting is "60" (seconds).

The number of seconds the site will allow a person to log in without entering the key or key+value after logging out.

As mentioned above, this was added after user requests. We suggest NOT using this feature.

Redirect URL

The default setting is {HOME}.

The {HOME} setting uses the Joomla API to determine what your homepage URL is, so you don't need to bother altering it when changing hosts or moving from development to production servers.

A complete URL is also valid, which may be local or remote.

A setting of {404} will return no session cookie, and will display a configurable 404 error template. The **404 Template** configuration will appear after {404} is typed into the Redirect URL field.

{404} is the safest, as it may confuse enough to cause an attacker to find another target. Any redirection may tip off an attacker that there's something there to attack.

404 Template

The default mimics a factory Apache 404 error page and is designed to fool an attacker into believing there is truly nothing to see. Actual server values are substituted into the template to make it more authentic. The template is as follows:

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL {url} was not found on this server.
<hr>
{serversignature}
</body></html>
```

- {url} and {serversignature} are replaced with the appropriate values obtained from the server

Frontend Restrictions

This is the second tab available within AdminExile configuration and is present for administrators who like to have certain users who are not allowed in the front-end. There are a variety of reasons for this, but to be succinct - if an administrative user account remains unknown to the outside world, it cannot be attacked.

By default, this feature is disabled as it could cause problems if automatically enabled. An administrator must explicitly turn it on, and must explicitly choose groups to restrict from front-end access. This is the ONLY front-end action that AdminExile takes.

- Restrict Frontend Groups: No
- Group Selection: <blank>

Setting "Restrict Frontend Groups" to "Yes" will display the "Group Selection" field.

Any member of a group chosen in "Group Selection" will be unable to log into the website frontend.

Mail Link

For many organizations, password expiration is something you can set your watch by. In a large organization with many administrative users, it may not be practical to contact everyone to inform them of the new AdminExile generated URL to access /administrator. This is where the Mail Link configurations can make life more simple. When enabled, an authorized /administrator user can enter a special URL which will trigger an email containing the current URL. No need to notify all of your users, the plugin can notify them for you.

- Enable Mail Link: Yes
- Mail Link Groups: [Super Users]

When enabled, any user who is a member of any of the "Mail Link Groups" is able to enter a URL which will trigger an email containing the /administrator URL.

This is the URL they will use: /administrator/?maillink=<username>

The plugin will look up the user, determine if they are a member of a group which is allowed to make this type of request and if so, email a link. Usernames which are not authorized are treated as any other invalid access - they are given the redirect option chosen on the Plugin tab.

IP Security

The ability to restrict by IP address was another feature added by popular demand. IP white and black lists capable of IPv4 and IPv6 addresses give administrators the ability to block individual troublemakers or entire networks from accessing /administrator while at the same time making things for convenient for users on trusted connections.

The IP security model used is Allow/Deny. Any address matching one defined in the white list is allowed access to /administrator without the key or key+value. Any address not on the white list and also on the black list is denied access to /administrator regardless of the key or key+value used. In other words, if you're on the white list - you're in. If you're on the black list - you're out. No exceptions.

Both lists are capable of understanding CIDR (Classless Inter-Domain Routing) netmask. This standardized network notation allows for greater flexibility when configuring the extension. If you need to block entire networks but are not familiar with CIDR netmasks, you can learn about them here: https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing (https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing)

The availability of IPv6 addresses depends on your PHP installation. If you have access to the entire GMP (GNU Multiple Precision) math library, then IPv6 addresses will be allowed within configuration. A message on the IP Security tab will inform you if the library and IPv6 are available or not. If it's not available, but you require it for your installation - you must contact your server administrator to install or enable it.
 http://php.net/manual/en/book.gmp.php (http://php.net/manual/en/book.gmp.php)

- Enable IP Security: "No"
- IP Whitelist: 127.0.0.1

- IP
  Blacklist: 10.0.0.0/8, 169.254.0.0/16, 172.16.0.0/12, 192.168.0.0/16
- Email Admin: "No"
- Email Once: "Yes"
- Email Recipient

Enable IP Security

When set to "No" all further configurations are ignored and no IP security actions are performed. Set to "Yes" to enable IP Security.

IP Whitelist

Add/Edit/Remove individual IP addresses or CIDR netmasks. Any address or network in this list will be allowed to access /administrator without key or key+value.

IP Blacklist

Add/Edit/Remove individual IP addresses or CIDR netmasks. Any address or network in this list will not be allowed to access /administrator with or without correct key or key+value. This table contains a counter showing how many attempts have been made by each entry.

Email Admin

If enabled, an email is sent to the configured user whenever a blacklisted address attempts access.

Email Once

If enabled, an email is sent to the configured user only the first time a blacklisted address attempts access.

Email Recipient

A user who is the intended recipient of IP Security notifications.

Brute Force

A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. (Techopedia)

AdminExile protects against brute force attacks in 3 ways:

1. Attempts to brute-force the key are counted
2. Attempts to brute-force the key+value are counted
3. If the correct key+value are passed, attempts to brute-force the /administrator login form are counted

Once an attacker reaches a threshold, they're blocked for a period of time. Subsequent attempts to access while blocked are ignored with the exception that they increase the period of time the attacker is blocked. There are 3 settings which govern how the brute force penalty is applied: Max Attempts (referred to as "max"), Time Penalty (referred to as "penalty") and Penalty Multiplier (referred to as "multiplier"). Here's an example of how it works with the settings max=5, penalty=5, multiplier=2:

1. An attacker makes 5 unsuccessful attempts to access /administrator, failing 5 key+value tests.
    - The attacker is given a 5 minute penalty where even if he guesses the right key+value - the plugin will not grant him access to the login form.
2. The attacker makes 1 more attempt during his 5 minute penalty
    - The penalty timer of 5 minutes is reset and multiplied by the multiplier.
    - The 5 minute penalty is now a 10 minute penalty and has re-started.

3. The attacker makes yet 1 more attempt during his newly reset 10 minute penalty.
    - The penalty timer of 10 minutes is reset and multiplied by the multiplier.
    - The 10 minute penalty is now a 20 minute penalty and has re-started.
4. The attacker makes yet 1 more attempt during his newly reset 20 minute penalty.
    - The penalty timer of 20 minutes is reset and multiplied by the multiplier.
    - The 20 minute penalty is now a 40 minute penalty and has re-started.

When considering that brute force attacks are generally undertaken by multiple computers simultaneously, with each system executing an attempt per second - the penalty can quickly grow to an impossible amount of time. The example above was only 8 attempts yielding 40 minutes of penalty. Three computers executing a brute force attack (once per second) for ten seconds using these settings would yield a penalty of 319 years. They're never getting in with brute force. AdminExile stopped them after just 5 attempts.

- Detect Brute Force: "No"
- Max Attempts: 5
- Time Penalty: 5
- Penalty Multiplier: 1
- Email Admin: "No"
- Email Once: "Yes"
- Email Recipient: <empty>

Detect Brute Force

The default is "No".

Setting to "Yes" enables the other fields on this tab. While set to "No", no brute force protection occurs.

Max Attempts

The default is 5

The number of unsuccessful attempts before a brute force is detected. Do not set this lower than 5. Standard Joomla logout redirects can trigger a brute-force detection if this setting is too low.

Time Penalty

The default is 5

The number of minutes applied as penalty when an attacker is identified. This penalty is used only once in the penalty phase. Further interactions with the same attacker are reset and multiplied.

Penalty Multiplier

The default is 1

The amount to multiply the current penalty when an attacker makes another attempt during his penalty period. The default is 1 for testing, but should be raised for production. 2 or 3 is recommended, although the sky is the limit.

Email Admin

The default is "No"

When an attacker is identified, or when he makes subsequent attempts - an the configured administrator is notified. Recommended to set to "Yes" once an email recipient is chosen.

Email Once

The default is "Yes"

When set to "Yes" the admin is notified only when the attacker is identified and penalized. This is the recommended setting, as attackers have no way of knowing that they have been penalized and may continue for hours or days.

Email Recipient

User who will receive brute-force emails.

HELP

Things go wrong. As much as we like my extensions to work perfectly, for everyone, all the time - people will still misconfigure the plugin, forget their keys, blacklist themselves, or get so many penalties against their IP address that they'll never get back in. We get click-happy sometimes too. Let's get you back up and running, shall we?

STOP! Don't delete anything! You can corrupt your system if you start deleting things. Joomla keeps records, and if you delete a file - you may not be able to purge the record of that file from the Joomla database.

This method for disabling the plugin requires access to your server filesystem. You only need to rename the same file twice. It's very easy. Follow this process step-by-step to ensure the integrity of your system.

1. Access your server filesystem in whatever means you normally use to browse the server files (FTP, SSH, FISH, CPanel).
    - Your access method needs to provide the ability to rename files.
2. Navigate to your Joomla website folders, into the plugins/system/adminexile directory.
3. Rename adminexile.php - you can rename it to anything, but I like adding an "X" to the filename, like this: Xadminexile.php.
    - I will refer to this filename later, so don't be confused if you renamed it to something else.
4. Once renamed, Joomla can't load this file - this means that AdminExile is no longer protecting your site.
    - Additionally, it means that it can't keep you locked out anymore!
5. Browse to your /administrator folder, into the Plugin Manager, and disable AdminExile.
6. Back in your server filesystem, rename Xadminexile.php back to adminexile.php.
    - By doing this, you can uninstall using the Extension Manager if

you so choose, or re-enable the plugin for use once the configuration issues are resolved.

The whole process should take only a few minutes.