

## CMS Made Simple Showtime2 module

### - Arbitrary file upload

It's possible use the image upload functionality for upload an arbitrary file such as a php script that can lead in code execution.

### Proof of Concept

- Login in admin panel on CMS Made Simple
- Go to Site Admin → Module Manager → Available Modules on “S” and install Showtime2 module:

Module Manager

Settings - Content Manager

Settings - Design Manager

Settings - File Manager

Settings - Global Settings

Settings - News module

System Maintenance




System Information

System Verification

Admin Log

Installed0 Upgrades AvailableSearchAvailable ModulesSettings

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Module Name	Version	Date	Downloads	Status/Action			
SelfRegistration	1.14.3	12/09/18	8872	Installed	Dependencies	Help	About
 SEOBoost	0.8.3beta	02/20/19	0	Installed	Dependencies	Help	About
 Showtime2	3.6.2	02/10/19	12039	Installed	Dependencies	Help	About
 SimpleSiteInfo	3.3	07/17/17	3424	Download & Install	Dependencies	Help	About

- Go to Content → Showtime2 Slideshow → Watermark Options tab and select a file to upload:

localhost/cmsms/admin/moduleinterface.php?mact=Showtime2,m1\_defaultadmin,0&\_c

### Showtime2 Slideshow

Show overview General Options Watermark Options

Upload new watermark image:

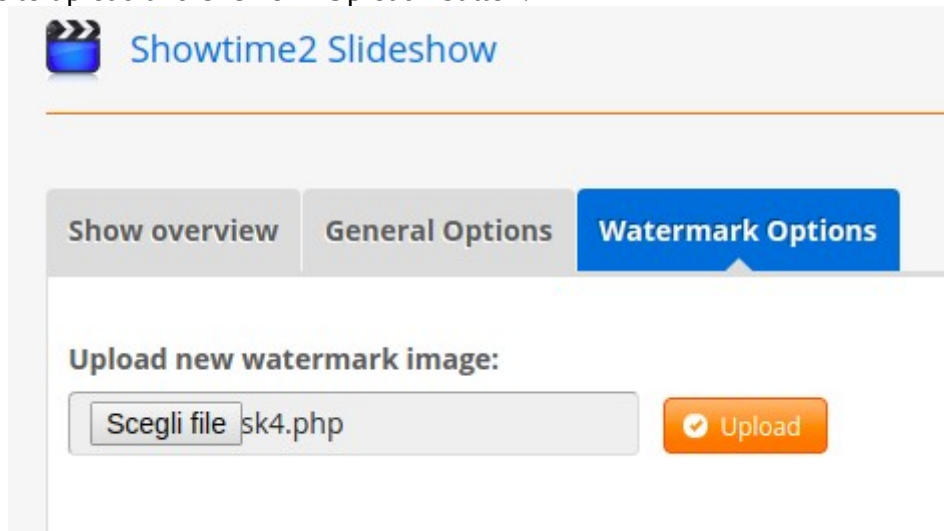
Scegli file Nessun file selezionato Upload

Nessun file selezionato

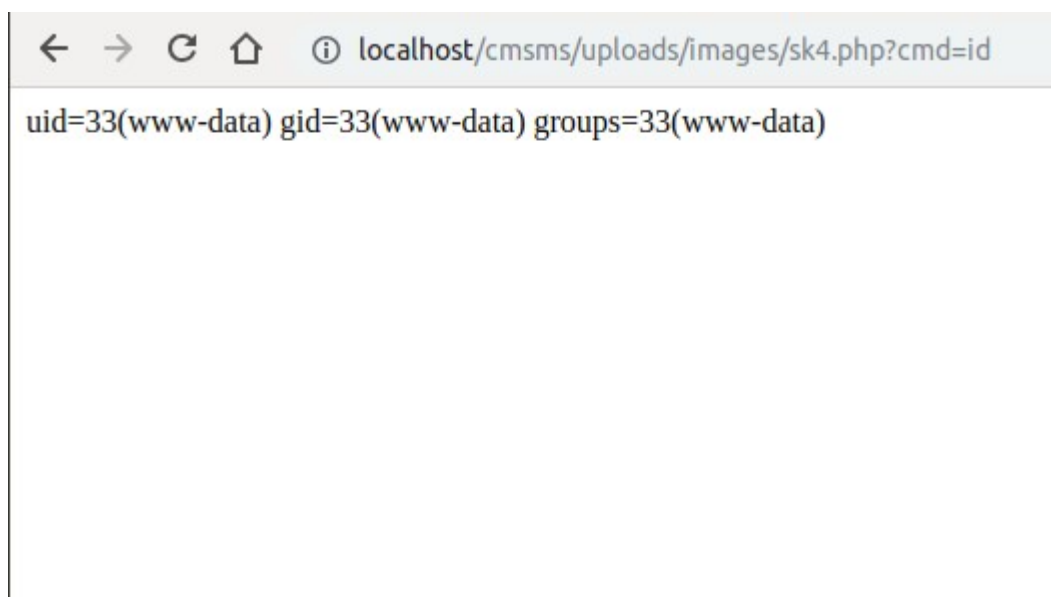
Current watermark (test.php)

Create bak-file when adding watermark

- Select a file to upload and click on “Upload” button:



- Now navigate in directory `uploads/images/SCRIPT_LOADED.php`:



### - SQL Injection

It's possible to obtain a SQL Injection in file `action.addpicture.php` with a crafted value in `m1_showid` parameter.

### Proof of Concept

- Login in admin panel on CMS Made Simple
- Send a GET request to:

`/moduleinterface.php?mact=Showtime2%2cm1_%2caddpicture%2c0&m1_showid=1+union+(select+sleep(10))&m1_sumbit&m1_filename`

with this payload the server sleeps for 10 seconds.

## - SQL Injection

It's possible to obtain a SQL Injection in file `class.showtime2_data.php` on function `_Getshowinfo` through `action.addslides.php` file with a crafted value on `m1_showid` parameter. Potentially also these functions are vulnerable to SQL Injection:

- `_updateshow` (parameter `show_id` e properties)
- `_inputshow` (parameter `show_id`)
- `_Getshowinfo` (parameter `show_id`)
- `_Getpictureinfo` (parameter `picture_id`)
- `_AdjustNameSeq` (parameter `shownumber`)
- `_Updatepicture` (parameter properties, `picture_id`, `whereclause`)
- `_Deletepicture` (parameter `picture_id`, `whereclause`)

## Proof of Concept

- Login in admin panel on CMS Made Simple
- Send a GET request to:

```
/moduleinterface.php?mact=Showtime2%2cm1_%2caddslides%2c0&m1_showid=1+union+
(select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,
34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,sleep(10))+--+
```