millken / doyocms Public

Code Issues 5 Pull requests Actions Projects Wiki Security ...

New issue

Jump to bottom

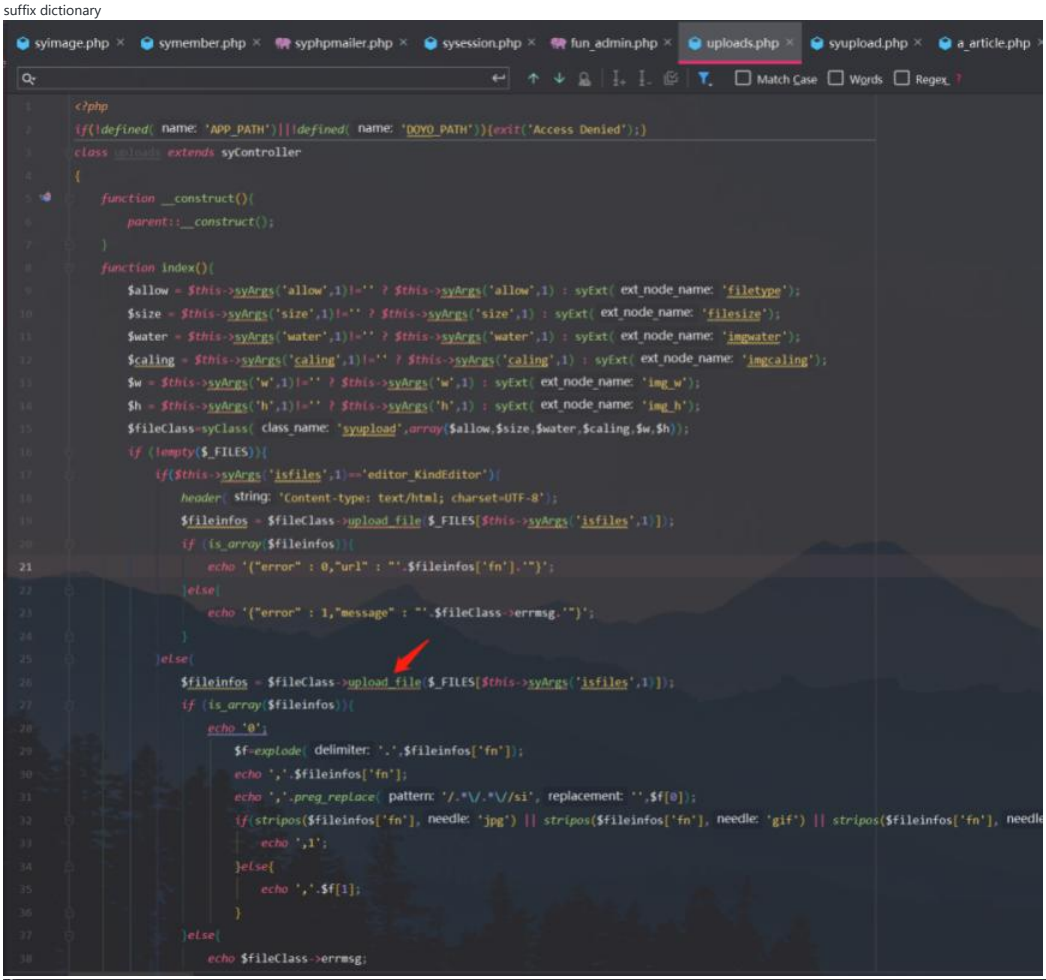
Vulnerabilities can be used to upload files of any type #4

Open jayus0821 opened this issue on Jan 31, 2021 · 0 comments

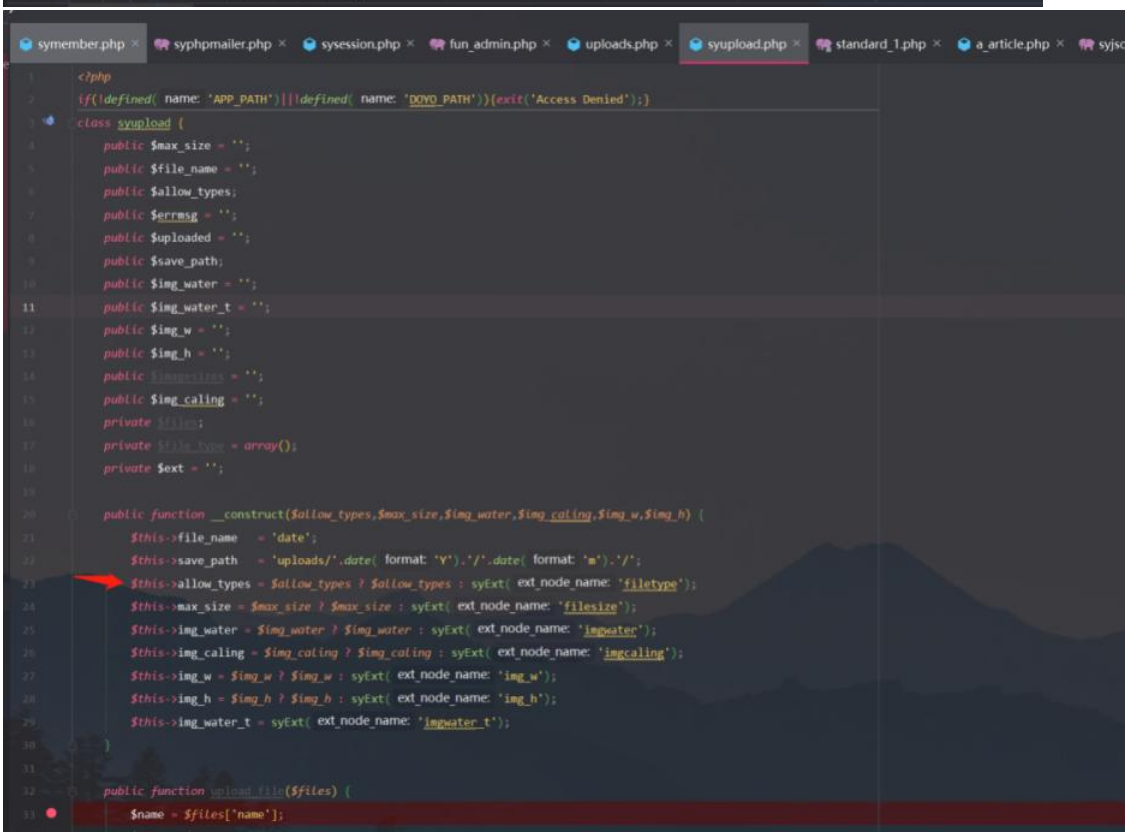
jayus0821 commented on Jan 31, 2021

in uploads.php

The first line receives the parameter allow, which is passed in when the syUpload object is instantiated, and when the syupload object is constructed, the passed allow is directly used as the allowed suffix dictionary



```php
<?php
if(!defined( name: 'APP_PATH')||!defined( name: 'DOYO_PATH')){exit('Access Denied');}
class uploads extends syController
{
    function __construct(){
        parent::__construct();
    }
    function index(){
        $allow = $this->syArgs('allow',1)!='' ? $this->syArgs('allow',1) : syExt( ext_node_name: 'filetype');
        $size = $this->syArgs('size',1)!='' ? $this->syArgs('size',1) : syExt( ext_node_name: 'filesize');
        $water = $this->syArgs('water',1)!='' ? $this->syArgs('water',1) : syExt( ext_node_name: 'imgwater');
        $caling = $this->syArgs('caling',1)!='' ? $this->syArgs('caling',1) : syExt( ext_node_name: 'imgcaling');
        $w = $this->syArgs('w',1)!='' ? $this->syArgs('w',1) : syExt( ext_node_name: 'img_w');
        $h = $this->syArgs('h',1)!='' ? $this->syArgs('h',1) : syExt( ext_node_name: 'img_h');
        $fileClass=syClass( class_name: 'syupload',array($allow,$size,$water,$caling,$w,$h));
        if (!empty($_FILES)){
            if($this->syArgs('isfiles',1)=='editor_KindEditor'){
                header( string: 'Content-type: text/html; charset=UTF-8');
                $fileinfos = $fileClass->upload_file($_FILES[$this->syArgs('isfiles',1)]);
                if (is_array($fileinfos)){
                    echo '{"error" : 0,"url" : "'.$fileinfos['fn'].'"}';
                }else{
                    echo '{"error" : 1,"message" : "'.$fileClass->errmsg.'"}';
                }
            }else{
                $fileinfos = $fileClass->upload_file($_FILES[$this->syArgs('isfiles',1)]);
                if (is_array($fileinfos)){
                    echo '0';
                        $f=explode( delimiter: '.',$fileinfos['fn']);
                        echo ','.$fileinfos['fn'];
                        echo ','.preg_replace( pattern: '/.*\/.*\//si', replacement: '',$f[0]);
                        if(stripos($fileinfos['fn'], needle: 'jpg') || stripos($fileinfos['fn'], needle: 'gif') || stripos($fileinfos['fn'], needle
                            echo ',1';
                        }else{
                            echo ','.$f[1];
                        }
                }else{
                    echo $fileClass->errmsg;
```

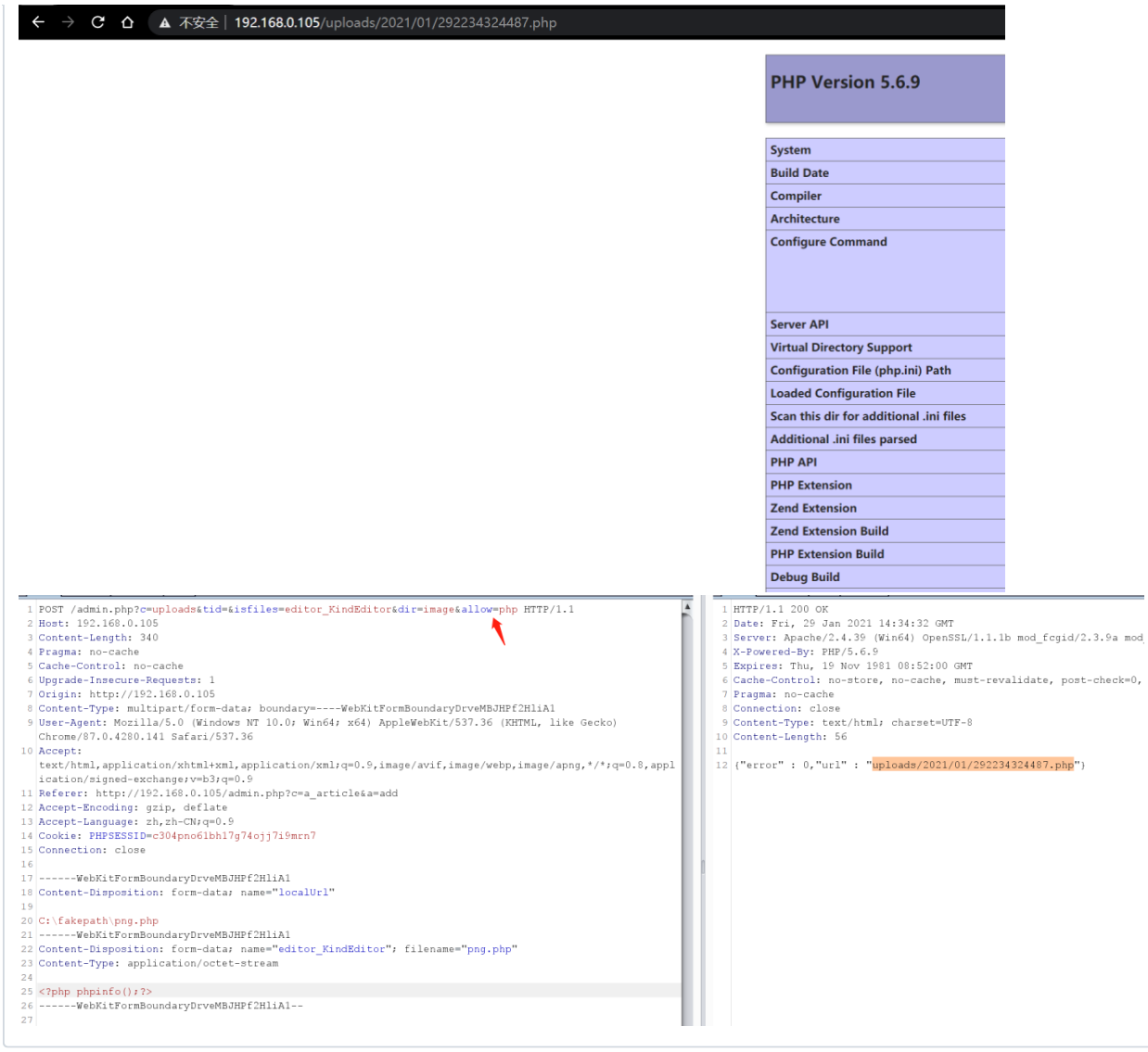


```php
<?php
if(!defined( name: 'APP_PATH')||!defined( name: 'DOYO_PATH')){exit('Access Denied');}
class syupload {
    public $max_size = '';
    public $file_name = '';
    public $allow_types;
    public $errmsg = '';
    public $uploaded = '';
    public $save_path;
    public $img_water = '';
    public $img_water_t = '';
    public $img_w = '';
    public $img_h = '';
    public $imagesizes = '';
    public $img_caling = '';
    private $files;
    private $file_type = array();
    private $ext = '';

    public function __construct($allow_types,$max_size,$img_water,$img_caling,$img_w,$img_h) {
        $this->file_name   = 'date';
        $this->save_path   = 'uploads/'.date( format: 'Y').'/'.date( format: 'm').'/';
        $this->allow_types = $allow_types ? $allow_types : syExt( ext_node_name: 'filetype');
        $this->max_size = $max_size ? $max_size : syExt( ext_node_name: 'filesize');
        $this->img_water = $img_water ? $img_water : syExt( ext_node_name: 'imgwater');
        $this->img_caling = $img_caling ? $img_caling : syExt( ext_node_name: 'imgcaling');
        $this->img_w = $img_w ? $img_w : syExt( ext_node_name: 'img_w');
        $this->img_h = $img_h ? $img_h : syExt( ext_node_name: 'img_h');
        $this->img_water_t = syExt( ext_node_name: 'imgwater_t');
    }

    public function upload_file($files) {
        $name = $files['name'];
```

So when we upload, we only need to add an allow parameter to upload files with any suffix



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant