The Code Execution Vulnerability of Ftcms

Exploit Title: Code execute

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 to use the background configuration modification function to modify the local config.php file is written. Next, analyze how to use it according to the code audit process.

First, locate the database configuration file code. The file location is admin/controllers/setting.php

```
1  http://host/admin/index.php/setting/setting_edit
```

The corresponding method of database configuration writing is setting_edit

admin/controllers/setting.php Plain Text Copy

```
    //设置配置变量(高级设置)
    public function setting_edit(){
           $data=$this->input->post();
       $res=$this->m->setting_edit($data['info']);
         if($res){
          $this->message('修改成功！',site_url($this->router->class.'/form'));
       }else{
          $this->message('修改失败！根目录config.php文件权限不够',site_url($this->r
outer->class.'/form'));
       }

    }

```

the first step,it use the $this->input->post() function of input class,get all data of post from user

then it use the setting_edit function in admin/models/settingm.php modify the config file，the code example:

Plain Text | Copy

```
//更新根目录config.php配置文件
 public function setting_edit($data){
        $res='';
  //循环分页配置
    $res.="//分页配置\r\n";
    foreach($data['wl_page'] as $key=>$v){
      $res=$res.'$GLOBALS["wl_page"]["'.$key.'"]='.$v.";\r\n";

    }

    //循环数据库配置
    $res.="//数据库配置\r\n";
    foreach($data['wl_db'] as $key=>$v){
       $res=$res.'$GLOBALS["wl_db"]["'.$key.'"]="'.$v.'".";\r\n";

    }

    //循环水印配置
    $res.="//水印信息配置\r\n";
    foreach($data['wl_water'] as $key=>$v){
       $res=$res.'$GLOBALS["wl_water"]["'.$key.'"]='.$v.";\r\n";
    }

     //编辑器远程图片自动下载
    $res.="//编辑器远程图片自动下载\r\n";
    foreach($data['wl_down'] as $key=>$v){
       $res=$res.'$GLOBALS["wl_down"]["'.$key.'"]='.$v.";\r\n";
    }
   //sdk
    $res.="//授权码，此授权码在软件初始化的时候自动生成，且唯一。请勿将此授权码告知其他客户。\r\n";
    foreach($data['wl_sdk'] as $key=>$v){
       $res=$res.'$GLOBALS["wl_sdk"]["'.$key.'"]="'.$v.'".";\r\n";
    }


     //循环调试信息配置
    $res.="//调试信息配置\r\n";
    foreach($data['wl_ts'] as $key=>$v){
      $res=$res.'$GLOBALS["wl_ts"]["'.$key.'"]='.$v.";\r\n";
    }

    $res="<?php \r\n".$res."\r\n?>";
    //写入信息
    $this->load->helper('file');
```

```
45      if ( ! write_file('../config.php', $res)){
47              return false;
48          }else{
49              return true;
50          }
51
    }
```

```
//循环水印配置
$res.="//水印信息配置\r\n";
foreach($data['wl_water'] as $key=>$v){
    $res=$res.'$GLOBALS["wl_water"]["'.$key.'"]='.$v.";\r\n";
}
```

You can see that this function will assign the passed value to the $res variable after traversal

```
$res="<?php \r\n".$res."\r\n?>";
```

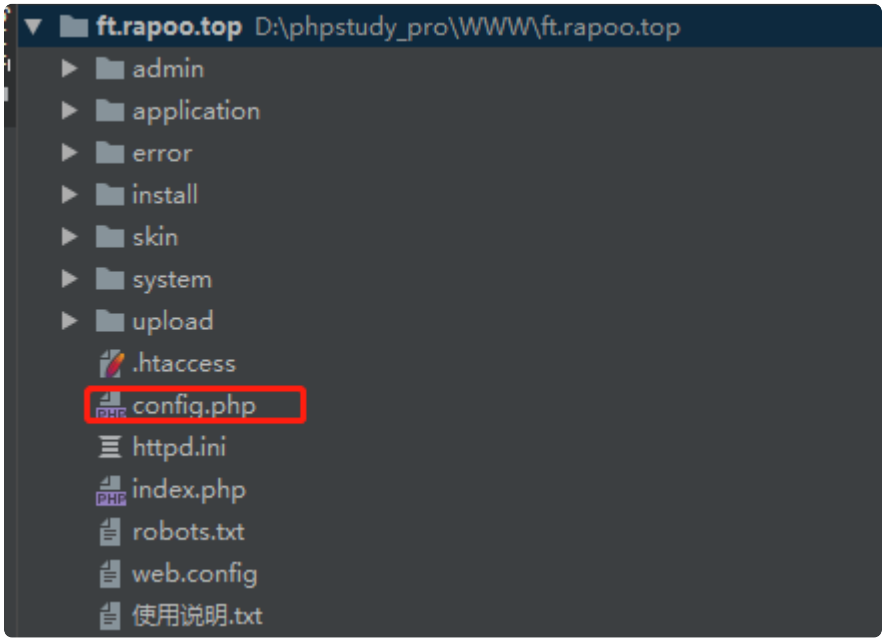
Then add the suffix of PHP file before and after the variable

```
//写入信息
$this->load->helper('file');
```

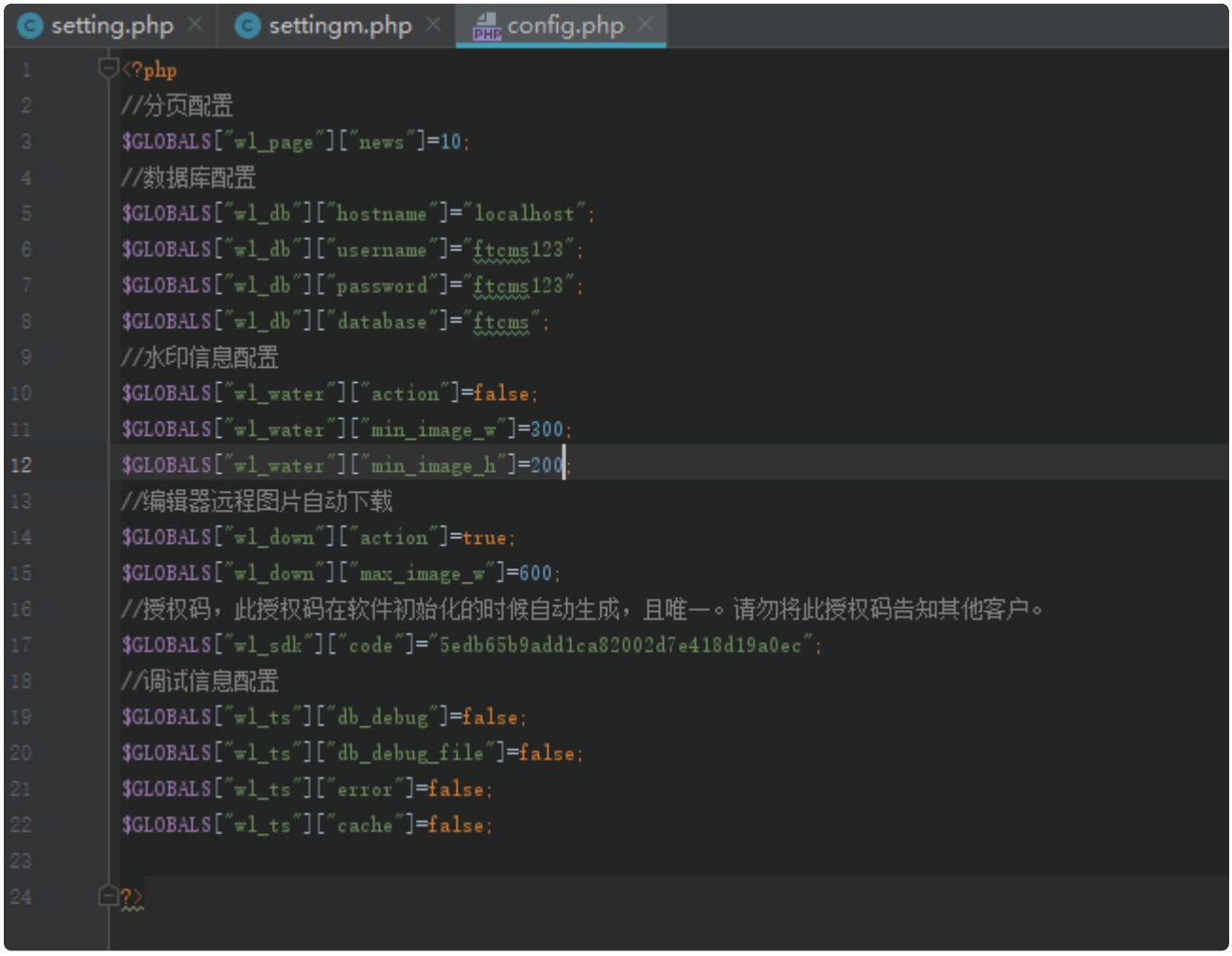
Then call the file class in the helper help class of CI framework

```
if ( ! write_file( path: '../config.php', $res)) {
    return false;
}else{
    return true;
}
```

Finally, call write_ The file function writes the contents of the spliced $res variable to the local config PHP file, and according to the website directory, config PHP is in the root directory of the website. The website structure is shown in the figure below:



Let's open config PHP file to check the file structure, which is helpful for us to construct POC and ensure the normal operation of the website



Because config The format in PHP is relatively standard, so we only need to use it; Separate them, and then splice the PHP code we need to execute. Here we choose the watermark information configuration, and the final POC is as follows

3.Loophole recurrence

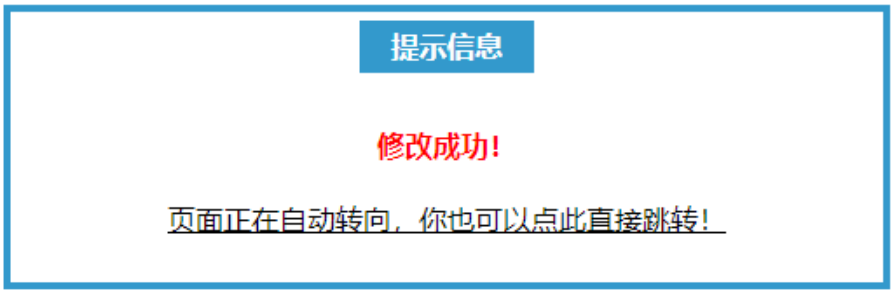
The complete data package is as follows

2.1 open the database config menu

Open background - Common - related configuration - website settings - Advanced Settings

2.2 Modify watermark settings

2.3 submit



2.4 request the config file

完整路径：

localhost/config.php

PHP Version 5.6.9

System	Windows NT DESKTOP-0UAEG7D 6.2 build 9200 (Windows 8 Enterprise Edition) AMD64
Build Date	May 13 2015 19:23:54
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x64\instantclient_12_1\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpstudy_pro\Extensions\php\php5.6.9nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS,VC11
PHP Extension Build	API20131226,NTS,VC11
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, sslv3, sslv2, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	convert.iconv.*, mcrypt.*, mdecrypt.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.6.0, Copyright (c) 1998-2015 Zend Technologies
with Xdebug v2.5.5, Copyright (c) 2002-2017, by Derick Rethans