

[New issue](#)[Jump to bottom](#)

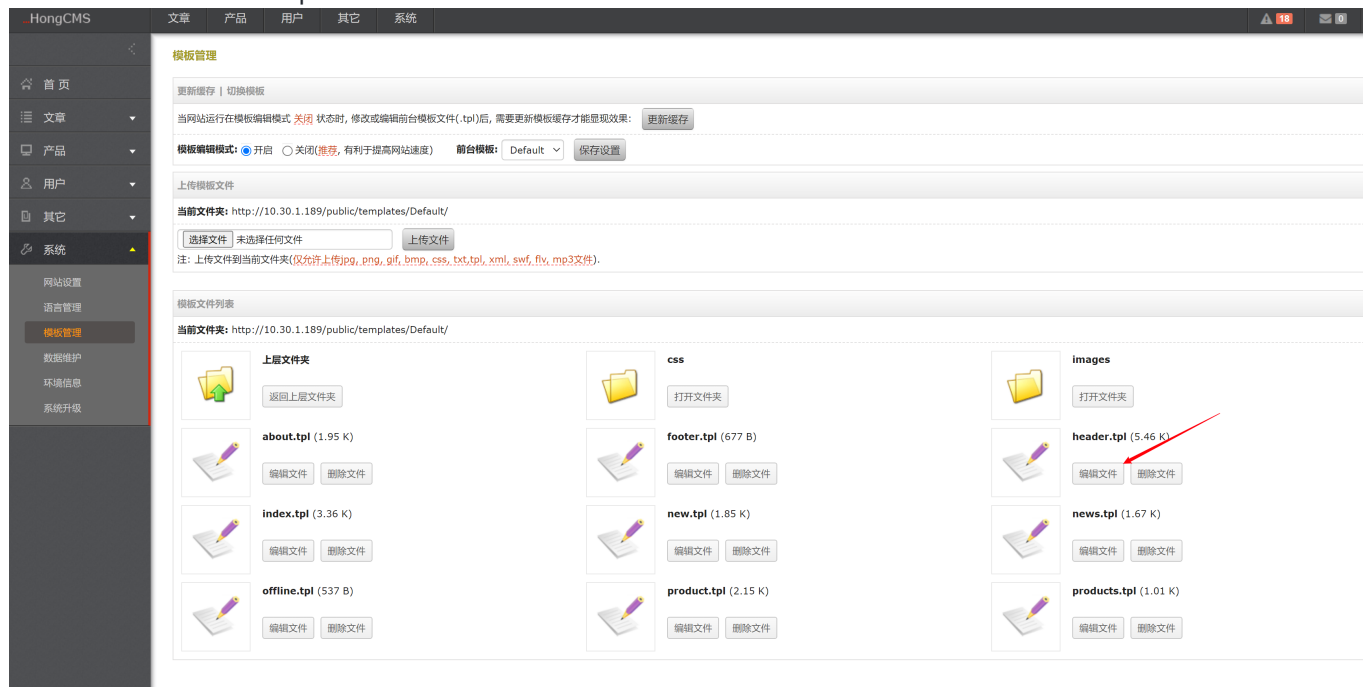
HongCMS 3.0 - Getshell by template/edit (Administrator Privilege) #19

[Open](#) Rixo1043 opened this issue on Jun 1 · 0 comments

Rixo1043 commented on Jun 1 • edited ▼

1.Login to the backstage as the administrator.

2.You need to edit the tpl file



3. Because the default safe mode configuration is off, so you can edit tpl file to getshell.
The vulnerability code is as follows:

```

3 //STpl模板类
4 class STpl{
5     var $_tpl_vars          = array();
6     var $tpl_left_delimiter = '{';
7     var $tpl_right_delimiter = '}';
8     var $tpl_template_dir   = 'templates/';
9     var $tpl_compile_dir     = 'cache/';
0     var $tpl_safe_mode = false;
1     var $tpl_check = true;
2
3     //编译
4     private function _compile($content){
5         $left_delimiter_quote = preg_quote($this->tpl_left_delimiter);
6         $right_delimiter_quote = preg_quote($this->tpl_right_delimiter);
7
8         //安全模式，替换php可执行代码
9         if($this->tpl_safe_mode){
10             $pattern="/\\<\\?.*\\?>/msUi";
11             $content = preg_replace($pattern, '<!-- PHP CODE REPLACED ON SAFE MODE -->', $content);
12         }
13
14         //替换注释: {xxxx*}
15         $pattern="/{$left_delimiter_quote}\\*(.*)\\*{$right_delimiter_quote}/msU";
16         $content = preg_replace($pattern, "<?php /*\\1*/?>", $content);
17
18         //调用_match函数编译
19         $pattern="/{$left_delimiter_quote}([\\S].*){$right_delimiter_quote}/msU";
20         return preg_replace_callback($pattern, array(&$this, '_match'), $content);
21     }
22
23     //清空当前模板缓存
24     public function clear_compiled_tpl(){
25         tpl_remove_cache($this->tpl_compile_dir);
26     }
27 }

```

5. Add you webshell code in tpl file.

The screenshot displays the HongCMS administration panel. On the left is a dark sidebar menu with options like '文章' (Articles), '产品' (Products), '用户' (Users), '其它' (Others), and '系统' (System). The '系统' option is selected, leading to a submenu where '模板管理' (Template Management) is highlighted.

The main area shows the '模板管理' (Template Management) page. At the top, it indicates the current file being edited: '当前文件: http://10.30.1.189/public/templates/Default/header.tpl'. Below this is a code editor displaying the HTML code for the header template. A red arrow points to a specific line in the code: '<% Poc is here %>'. The code includes various PHP and HTML tags for language switching, user authentication, and site navigation.

The screenshot shows a web browser window with the address bar displaying '172.26.2.174/?a=phpinfo()'. The page content includes the PHP version '5.4.45' and the 'php' logo. A red arrow points to the text '<% Poc is here %>' in the browser's status bar, indicating the successful execution of the PoC. The page also features a '首页' (Home) button and a search bar.

- 1、 Set safe mode true by default.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

